McAfee®

Wireless Protection 2007

Guia do Usuário

Conteúdo

CAPÍTULO 1

McAfee Wireless Protection

O McAfee Wireless Protection Suite elimina as inconveniências do trabalho em rede e os riscos de segurança das redes sem fio. Sua proteção confiável impede que hackers ataquem a sua rede Wi-Fi®, protege suas transações e informações pessoais e não permite que outras pessoas usem a sua rede para acessar a Internet; tudo isso com apenas um único clique. As chaves de criptografia fortes e em rotação do McAfee Wireless Network Security frustram até os intrusos sem fio mais determinados. O Wireless Protection também inclui o McAfee EasyNetwork, que simplifica o compartilhamento de arquivos e impressoras em sua rede. Além disso, ele é fornecido com o McAfee Network Manager, que monitora computadores em toda a sua rede, procurando por fragilidades de segurança, e facilita a correção de problemas de segurança em potencial.

O Wireless Protection inclui os seguintes programas:

- SecurityCenter
- Wireless Network Security
- Network Manager
- EasyNetwork

CAPÍTULO 2

McAfee SecurityCenter

O McAfee SecurityCenter é um ambiente fácil de usar, no qual os usuários da McAfee podem iniciar, gerenciar e configurar suas assinaturas de segurança.

O SecurityCenter também funciona como uma fonte de informações sobre alertas de vírus, produtos, suporte, assinaturas e como acesso com um único clique às ferramentas e às notícias do site da McAfee na Web.

Neste capítulo

Recursos

O McAfee SecurityCenter possui os seguintes novos recursos e benefícios:

Status de proteção reprojetado

Analise facilmente o status da segurança do computador, verifique se há atualizações e corrija potenciais problemas de segurança.

Upgrades e atualizações contínuos

Instalação automática de atualizações diárias. Quando há uma nova versão do software McAfee disponível, você a recebe automaticamente sem custo adicional durante sua assinatura, garantindo que você sempre tenha a proteção mais recente.

Alertas em tempo real

Os alertas de segurança notificam sobre epidemias de vírus emergenciais e ameaças à segurança. Também oferecem opções de resposta para remover, neutralizar ou aprender mais sobre a ameaça.

Proteção conveniente

Diversas opções de renovação ajudam a manter sua proteção McAfee atualizada.

Ferramentas de desempenho

Remova arquivos não utilizados, desfragmente arquivos utilizados e use a restauração do sistema para manter seu computador funcionando com o máximo de desempenho.

Ajuda on-line real

Obtenha suporte de especialistas em segurança de computador da McAfee, via bate-papo na Internet, e-mail e telefone.

Proteção de navegação segura

Quando instalado, o plug-in para navegador do McAfee SiteAdvisor ajuda a proteger contra spyware, spam, vírus e fraudes on-line, classificando sites da Web que você visita ou que aparecem em seus resultados de pesquisa na Web. Você pode exibir classificações de segurança detalhadas para mostrar os resultados dos testes do site em relação a práticas de e-mail, downloads, afiliações on-line e inconvenientes como pop-ups e cookies de rastreamento de terceiros.

CAPÍTULO 3

Usando o SecurityCenter

Você pode executar o SecurityCenter a partir do ícone do McAfee SecurityCenter na área de notificação do Windows na extrema direita da barra de tarefas, ou na área de trabalho do Windows.

Quando o SecurityCenter é aberto, o painel Início exibe o status da segurança do computador e fornece acesso rápido a atualizações, varredura (se o McAfee VirusScan estiver instalado) e outras tarefas comuns:

Cabeçalho

Ajuda

Exibir o arquivo de Ajuda do programa.

Coluna esquerda

Atualizar

Atualize seu produto para se proteger contra as ameaças mais recentes.

Varredura

Se o McAfee VirusScan estiver instalado, você poderá executar uma varredura manual em seu computador.

Tarefas comuns

Execute tarefas comuns, incluindo retornar ao painel Início, exibir eventos recentes, gerenciar a rede do computador (se for um computador com recursos de gerenciamento para esta rede) e manutenção do computador. Se o McAfee Data Backup estiver instalado, você também poderá fazer backup de dados.

Componentes instalados

Veja quais serviços de segurança estão protegendo seu computador.

Painel principal

Status de proteção

Em **Estou protegido?**, consulte o nível geral do status de proteção do computador. Abaixo desta opção, exiba uma análise do status por categoria ou tipo de proteção.

Informações do SecurityCenter

Veja quando ocorreu a última atualização de seu computador, quando ocorreu a última varredura (se o McAfee VirusScan estiver instalado), além da data de expiração da assinatura.

Neste capítulo

Noções básicas sobre os ícones do SecurityCenter

Os ícones do SecurityCenter aparecem na área de notificação do Windows, na extrema direita da barra de tarefas. Use-os para saber se seu computador está totalmente protegido, para exibir o status de uma varredura em andamento (se o McAfee VirusScan estiver instalado), verificar atualizações, exibir eventos recentes, fazer a manutenção do computador e para obter suporte no site da McAfee na Web.

Abra o SecurityCenter e use recursos adicionais

Quando o SecurityCenter está sendo executado, o ícone M do SecurityCenter aparece na área de notificação do Windows, na extrema direita da barra de tarefas.

Para abrir o SecurityCenter ou usar recursos adicionais:

- Clique com o botão direito no ícone principal do SecurityCenter e clique em uma das seguintes opções:
  - Abrir o SecurityCenter
  - Atualizações
  - Links rápidos

    O submenu contém links para Início, Exibir eventos recentes, Gerenciar rede, Manter o computador e para o Data Backup (se estiver instalado).
  - Verificar assinatura

    (Esse item aparece quando a assinatura de ao menos um produto tiver expirado.)
  - Centro de Upgrade
  - Suporte ao cliente

Verifique o status de proteção

Quando o computador não está totalmente protegido, o ícone do status de proteção aparece na área de notificação do Windows, na extrema direita da barra de tarefas. O ícone pode ser amarelo ou vermelho, dependendo do status de proteção.

Para verificar o status de proteção:

- Clique no ícone do status de proteção para abrir o SecurityCenter e corrigir qualquer problema.

Verifique o status das atualizações

Quando o você verifica atualizações, o ícone de atualização aparece na área de notificação do Windows, na extrema direita da barra de tarefas.

Para verificar o status das atualizações:

- Aponte para o ícone de atualizações para exibir o status de suas atualizações em uma dica.

Noções básicas sobre o status de proteção

O status de proteção de segurança geral do computador é mostrado em **Estou protegido?** no SecurityCenter.

O status de proteção informa se o computador está totalmente protegido contra as ameaças à segurança mais recentes ou se os problemas requerem atenção e como resolvê-los. Quando um problema afeta mais de uma categoria de proteção, a correção do problema pode fazer com que várias categorias retornem ao status de proteção total.

Alguns dos fatores que influenciam o status de proteção são ameaças externas à segurança, os produtos de segurança instalados no computador, produtos que acessam a Internet e a forma como esses produtos de segurança e de Internet estão configurados.

Por padrão, se a Proteção contra spam ou o Bloqueio de conteúdo não estiverem instalados, esses problemas de proteção menos importantes serão ignorados automaticamente e não serão rastreados no status de proteção geral. Porém, se um problema de proteção for seguido de um link **Ignorar**, você poderá optar por ignorar o problema, se tiver certeza de que não deseja corrigi-lo.

Estou protegido?

Consulte o nível geral do status de proteção do computador em **Estou protegido?** no SecurityCenter:

- A mensagem **Sim** será exibida se seu computador estiver totalmente protegido (verde).
- A mensagem **Não** será exibida se seu computador estiver parcialmente protegido (amarelo) ou não estiver protegido (vermelho).

Para resolver automaticamente a maioria dos problemas de proteção , clique em **Corrigir** ao lado do status de proteção. Porém, se um ou mais problemas persistirem e exigirem sua resposta, clique no link exibido junto ao problema para adotar a ação sugerida.

Noções básicas sobre as categorias e tipos de proteção

Em **Estou protegido?** no SecurityCenter, você pode exibir uma análise do status consistindo nos seguintes tipos e categorias de proteção:

- Computador e arquivos
- Internet e rede
- E-mail e mensagens instantâneas
- Controles pelos pais

Os tipos de proteção exibidos no SecurityCenter dependem de quais produtos estão instalados. Por exemplo, o tipo de proteção PC Health é exibido se o software McAfee Data Backup estiver instalado.

Se uma categoria não tiver problemas de proteção, o status será verde. Se você clicar em uma categoria verde, uma lista dos tipos de proteção ativados será exibida à direita, seguida de uma lista de problemas já ignorados. Se não houver nenhum problema, um comunicado sobre o vírus será exibido no lugar dos problemas. Você também pode clicar em **Configurar** para alterar as opções para essa categoria.

Se todos os tipos de proteção em uma categoria tiverem status verde, então o status da categoria será verde. Do mesmo modo, se todas as categorias de proteção tiverem status verde, então o Status de proteção geral será verde.

Se alguma das categorias de proteção tiver status amarelo ou vermelho, você poderá resolver os problemas de proteção corrigindo-os ou ignorando-os e, assim, o status será alterado para verde.

Noções básicas sobre a proteção para Computador e arquivos

A categoria de proteção Computador e arquivos consiste nos seguintes tipos de proteção:

- **Proteção contra vírus** -- A proteção da varredura em tempo real defende o computador contra vírus, worms, cavalos de Tróia, scripts suspeitos, ataques híbridos e outras ameaças. Ela faz a varredura automaticamente e tenta limpar arquivos (inclusive arquivos .exe compactados, arquivos do setor de inicialização, da memória e arquivos importantes) quando são acessados por você ou pelo computador.
- **Proteção contra spyware** -- A proteção contra spyware detecta, bloqueia e remove rapidamente spyware, adware e outros programas potencialmente indesejados que podem coletar e transmitir os seus dados particulares sem a sua permissão.
- **SystemGuards** -- Os SystemGuards detectam alterações em seu computador e alertam você quando elas ocorrem. Você pode conferir essas alterações e decidir permiti-las ou não.
- **Proteção do Windows** -- A proteção do Windows informa o status do Windows Update em seu computador. Se o McAfee VirusScan estiver instalador, a proteção contra a sobrecarga do buffer também estará disponível.

Um dos fatores que influenciam a proteção Computador e arquivos é a ameaça externa de vírus. Por exemplo, se ocorrer uma epidemia de vírus, o seu software antivírus o protegerá? Além disso, há outros fatores, dentre eles a configuração do software antivírus e se o software é atualizado continuamente com os arquivos de detecção de assinatura mais recentes, para proteger o computador das últimas ameaças.

Abrir o painel de configuração Computador e arquivos

Quando não houver problemas em **Computador & arquivos**, você poderá abrir o painel de configuração a partir do painel de informações.

Para abrir o painel de configuração Computador e arquivos:

1. No painel Início, clique em **Computador & arquivos**.
2. No painel direito, clique em **Configurar**.

Noções básicas sobre a proteção de Internet e rede

A categoria de proteção Internet e rede consiste nos seguintes tipos de proteção:

- **Proteção de firewall** -- A proteção de firewall defende o computador contra invasão e tráfego de rede não desejado. Ela ajuda a gerenciar conexões de entrada e de saída com a Internet.
- **Wireless Protection** -- A Wireless Protection defende a rede sem fio doméstica contra intrusão e interceptação de dados. No entanto, se, no momento, você estiver conectado a uma rede sem fio externa, a proteção deve variar com base no nível de segurança dessa rede.
- **Proteção de navegação na Web** -- A proteção da navegação da Web oculta anúncios, pop-ups e Web bugs em seu computador quando você navega pela Internet.
- **Proteção contra phishing** -- A proteção contra phishing ajuda a bloquear sites fraudulentos que solicitam informações pessoais por meio de hiperlinks em e-mails, mensagens instantâneas, pop-ups e outras fontes.
- **Proteção de informações pessoais** -- A proteção de informações pessoais bloqueia a divulgação de informações importantes e confidenciais pela Internet.

Abrir o painel de configuração de Internet e rede

Quando não houver problemas em **Internet & rede**, você poderá abrir o painel de configuração a partir do painel de informações.

Para abrir o painel configuração de Internet e rede:

1. No painel Início, clique em **Internet & rede**.
2. No painel direito, clique em **Configurar**.

Noções básicas sobre a proteção E-mail e MI

A categoria de proteção E-mail e MI consiste nos seguintes tipos de proteção:

- **Proteção de e-mail** -- A proteção de e-mail faz a varredura automaticamente e tenta limpar vírus, spyware e ameaças potenciais em e-mails de entrada e de saída e em anexos.
- **Proteção contra spam** -- A proteção contra spam ajuda a bloquear a entrada de mensagens de e-mail indesejadas em sua caixa de entrada.
- **Proteção de MI** -- A proteção para mensagens instantâneas (MI) faz a varredura automaticamente e tenta limpar vírus, spyware e ameaças potenciais em anexos de mensagens instantâneas de entrada. Ela também impede que clientes de mensagens instantâneas compartilhem conteúdo indesejado ou informações pessoais na Internet.
- **Proteção para navegação segura** -- Quando instalado, o plug-in para navegador do McAfee SiteAdvisor ajuda a proteger contra spyware, spam, vírus e golpes on-line, classificando sites da Web que você visita ou que aparecem em seus resultados de pesquisa na Web. Você pode exibir classificações de segurança detalhadas para mostrar os resultados dos testes do site em relação a práticas de e-mail, downloads, afiliações on-line e inconvenientes como pop-ups e cookies de rastreamento de terceiros.

Abrir o painel de configuração de E-mail e MI

Quando não houver problemas em **E-mail & MI**, você poderá abrir o painel de configuração a partir do painel de informações.

Para abrir o painel de configuração de E-mail e MI:

1. No painel Início, clique em **E-mail & MI**.
2. No painel direito, clique em **Configurar**.

Noções básicas sobre a proteção Controles pelos pais

A categoria de proteção Controles pelos pais consiste no seguinte tipo de proteção:

- **Controles pelos pais** -- O Bloqueio de conteúdo impede que usuários exibam conteúdo indesejado da Internet, bloqueando sites da Web potencialmente mal-intencionados. O uso e as atividades na Internet dos usuários também podem ser monitorados e limitados.

Abrir o painel de configuração Controles pelos pais

Quando não houver problemas em **Controles pelos pais**, você poderá abrir o painel de configuração a partir do painel de informações.

Para abrir o painel de configuração Controles pelos pais:

1. No painel Início, clique em **Controles pelos pais**.
2. No painel direito, clique em **Configurar**.

Corrigindo problemas de proteção

A maior parte dos problemas de proteção pode ser resolvida automaticamente. Porém, se um ou mais problemas persistirem, você deverá resolvê-los.

Corrigir problemas de proteção automaticamente

A maior parte dos problemas de proteção pode ser resolvida automaticamente.

Para corrigir problemas de proteção automaticamente:

- Clique em **Corrigir**, ao lado do status de proteção.

Corrigir problemas de proteção manualmente

Se um ou mais problemas de proteção não forem resolvidos automaticamente, clique no link ao lado do problema para adotar a ação sugerida.

Para corrigir problemas de proteção manualmente:

- Escolha uma das seguintes opções:
    - Se não tiver sido feita uma varredura completa de seu computador nos últimos 30 dias, clique em **Varredura** à esquerda do status de proteção principal, para realizar uma varredura manual. (Esse item aparecerá se o McAfee VirusScan estiver instalado.)
    - Se os seus arquivos de detecção de assinatura (DAT) estiverem desatualizados, clique no link **Atualizar**, à esquerda do status de proteção principal, para atualizar sua proteção.
    - Se o programa não estiver instalado, clique em **Obter proteção total** para instalá-lo.
    - Se um programa estiver com componentes faltantes, reinstale-o.
    - Se um programa precisar ser registrado para receber proteção total, clique em **Registrar agora**, para registrá-lo. (Esse item aparece quando um ou mais programas expiraram.)
    - Se um programa expirar, clique em **Verificar minha assinatura agora**, para verificar o status de sua conta. (Esse item aparece quando um ou mais programas expiraram.)

Exibindo informações do SecurityCenter

Na parte inferior do painel de status de proteção, as Informações do SecurityCenter fornecem acesso às opções do SecurityCenter e mostram a última atualização, a última varredura (se o McAfee VirusScan estiver instalado) e informações sobre expiração de assinatura dos produtos McAfee.

Abra o painel de configuração do SecurityCenter

Para maior praticidade, você pode abrir o painel de configuração do SecurityCenter para alterar as opções, a partir do painel Início.

Para abrir o painel de configuração do SecurityCenter:

- No painel Início, em **Informações do SecurityCenter**, clique em **Configurar**.

Exiba as informações do produto instalado

Você pode exibir uma lista de produtos instalados que mostra o número da versão do produto e a data da última atualização.

Para exibir as informações do produto McAfee:

- No painel Início, em **Informações do SecurityCenter**, clique em **Exibir detalhes** para abrir a janela de informações do produto.

Usando o Menu avançado

Quando o SecurityCenter é aberto pela primeira vez, o Menu básico aparece na coluna à esquerda. Se você for um usuário avançado, pode clicar no **Menu avançado** para abrir um menu de comandos mais detalhado no lugar desse. Para maior praticidade, o último menu usado será mostrado dá próxima vez que você abrir o SecurityCenter.

O Menu avançado contém os seguintes itens:

- Início
- Relatórios e registros (inclui a lista de Eventos recentes e registros por tipo dos últimos 30, 60 e 90 dias)
- Configurar
- Restaurar
- Ferramentas

CAPÍTULO 4

Configurando opções do SecurityCenter

O SecurityCenter mostra o status de proteção de segurança geral do computador, permite criar contas de usuário McAfee, instala automaticamente as atualizações mais recentes do produto e notifica você automaticamente, com alertas e sons, sobre epidemias públicas de vírus, ameaças à segurança e atualizações do produto.

No painel de configuração do SecurityCenter, é possível alterar as opções do SecurityCenter para os seguintes recursos:

- Status de proteção
- Usuários
- Atualizações automáticas
- Alertas

Neste capítulo

Configurando o status de proteção

O status de proteção de segurança geral do computador é mostrado em **Estou protegido?** no SecurityCenter.

O status de proteção informa se o computador está totalmente protegido contra as ameaças à segurança mais recentes ou se os problemas requerem atenção e como resolvê-los.

Por padrão, se a Proteção contra spam ou o Bloqueio de conteúdo não estiverem instalados, esses problemas de proteção menos importantes serão ignorados automaticamente e não serão rastreados no status de proteção geral. Porém, se um problema de proteção for seguido de um link **Ignorar**, você poderá optar por ignorar o problema, se tiver certeza de que não deseja corrigi-lo. Se, posteriormente, decidir corrigir um problema ignorado anteriormente, você poderá incluí-lo no status de proteção para rastreamento.

Configurar problemas ignorados

Você pode incluir ou excluir problemas do rastreamento como parte do status de proteção geral do computador. Se um problema de proteção for seguido por um link **Ignorar**, você poderá optar por ignorar o problema, se tiver certeza de que não deseja corrigi-lo. Se, posteriormente, decidir corrigir um problema ignorado anteriormente, você poderá incluí-lo no status de proteção para rastreamento.

Para configurar problemas ignorados:

1 Em **Informações do SecurityCenter**, clique em **Configurar**.

2 Clique na seta ao lado de **Status de proteção** para expandir o painel e clique em **Avançado**.

3 Realize uma das seguintes ações no painel Problemas ignorados:

   - Para incluir problemas ignorados anteriormente no status de proteção, desmarque suas caixas de seleção.
   - Para excluir problemas do status de proteção, selecione suas caixas de seleção.

4 Clique em **OK**.

Configurando opções do usuário

Se você estiver executando programas da McAfee que exigem permissões de usuário, essas permissões corresponderão, por padrão, às contas de usuário do Windows em seu computador. Para facilitar o gerenciamento de usuários para esses programas, você pode alternar para usar contas de usuário da McAfee a qualquer momento.

Se você alternar para as contas de usuário da McAfee, todos os nomes de usuário e permissões existentes no programa Controles pelos pais serão importados automaticamente. No entanto, na primeira vez em que você alterna, é necessário criar uma Conta de administrador. Depois disso, você pode começar a criar e configurar outras contas de usuário da McAfee.

Alternar para contas de usuário da McAfee

Por padrão, você usa contas de usuário do Windows. No entanto, alternar para contas de usuário da McAfee faz com que seja desnecessário criar contas adicionais de usuário do Windows.

Para alternar para contas de usuário da McAfee:

1 Em **Informações do SecurityCenter**, clique em **Configurar**.

2 Clique na seta ao lado de **Usuários** para expandir o painel e clique em **Avançado**.

3 Para usar contas de usuário da McAfee, clique em **Alternar**.

Caso esteja alternando para contas de usuário da McAfee pela primeira vez, você deve criar uma Conta de administrador (página 24).

Criar uma Conta de administrador

Na primeira vez em que alternar para utilizar usuários da McAfee, você receberá uma solicitação para criar uma Conta de administrador.

Para criar uma Conta de administrador:

1 Digite uma senha na caixa **Senha** e digite-a novamente na caixa **Confirmar senha**.

2 Selecione uma pergunta de recuperação de senha da lista e digite a resposta à pergunta secreta na caixa **Resposta**.

3 Clique em **Aplicar**.

Quando você concluir, o tipo de conta do usuário estará atualizado no painel, com os nomes de usuário e as permissões existentes do programa Controles pelos pais, se houver. Se você estiver configurando contas de usuário pela primeira vez, o painel Gerenciar usuários será exibido.

Configurar opções do usuário

Se você alternar para as contas de usuário da McAfee, todos os nomes de usuário e permissões existentes no programa Controles pelos pais serão importados automaticamente. No entanto, na primeira vez em que você alterna, é necessário criar uma Conta de administrador. Depois disso, você pode começar a criar e configurar outras contas de usuário da McAfee.

Para configurar opções do usuário:

1 Em **Informações do SecurityCenter**, clique em **Configurar**.

2 Clique na seta ao lado de **Usuários** para expandir o painel e clique em **Avançado**.

3 Em **Contas de usuário**, clique em **Adicionar**.

4 Digite um nome de usuário na caixa **Nome do usuário**.

5 Digite uma senha na caixa **Senha** e digite-a novamente na caixa **Confirmar senha**.

6 Selecione a caixa **Usuário de inicialização**, se desejar que este usuário efetue logon automaticamente quando o SecurityCenter for iniciado.

7 Em **Tipo de conta de usuário**, selecione um tipo de conta para este usuário e clique em **Criar**.

Observação: Após criar a conta de usuário, você deve definir as configurações para um Usuário limitado em Controles pelos pais.

8 Para editar a senha, o logon automático ou o tipo de conta de um usuário, selecione um nome de usuário na lista e clique em **Editar**.

9 Ao terminar, clique em **Aplicar**.

Recuperar a Senha de administrador

Caso esqueça a Senha do administrador, você poderá recuperá-la.

Para recuperar a senha de administrador:

1 Clique com o botão direito do mouse no ícone M do SecurityCenter e clique em **Alternar usuário**.

2 Na lista **Nome do usuário**, selecione **Administrador** e clique em **Esqueceu a senha?**.

3 Digite a resposta à pergunta secreta que você selecionou ao criar a Conta do administrador.

4 Clique em **Enviar**.

A Senha do administrador esquecida será exibida.

Alterar a Senha do administrador

Caso não consiga lembrar a Senha do administrador ou suspeite que ela esteja comprometida, você pode alterá-la.

Para alterar a Senha do administrador:

1 Clique com o botão direito do mouse no ícone M do SecurityCenter e clique em **Alternar usuário**.
2 Na lista **Nome do usuário**, selecione **Administrador** e clique em **Alterar senha**.
3 Digite a senha atual na caixa **Senha antiga**.
4 Digite sua nova senha na caixa **Senha**, e digite-a novamente na caixa **Confirmar senha**.
5 Clique em **OK**.

Configurando opções de atualização

O McAfee SecurityCenter verifica automaticamente se há atualizações para todos os serviços McAfee a cada quatro horas, quando você está conectado à Internet, instalando automaticamente as atualizações mais recentes do produto. Porém, você pode verificar atualizações manualmente a qualquer momento, usando o ícone do SecurityCenter na área de notificação na extrema direita da barra de tarefas.

Verificar atualizações automaticamente

O SecurityCenter verifica automaticamente as atualizações a cada quatro horas quando você está conectado à Internet. No entanto, você pode configurar o SecurityCenter para notificar você antes de fazer download ou instalar atualizações.

Para verificar atualizações automaticamente:

1 Em **Informações do SecurityCenter**, clique em **Configurar**.

2 Clique na seta ao lado do status de **Atualizações automáticas ativadas** para expandir o painel e clique em **Avançado**.

3 Selecione uma das opções a seguir, no painel Opções de atualização:

- Instalar as atualizações automaticamente e notificar-me quando o produto estiver atualizado (recomendável) (página 28)
- Fazer o download das atualizações automaticamente e notificar-me quando estiverem prontas para serem instaladas (página 29)
- Notificar-me antes de fazer o download de atualizações (página 29)

4 Clique em **OK**.

Observação: Para obter proteção máxima, a McAfee recomenda que você deixe o SecurityCenter verificar e instalar as atualizações automaticamente. Entretanto, se desejar atualizar apenas manualmente os serviços de segurança, você poderá desativar a atualização automática (página 30).

Fazer o download e a instalação das atualizações automaticamente

Se você selecionar **Instalar as atualizações automaticamente e notificar-me quando meus serviços forem atualizados (recomendável)**, nas Opções de atualização do SecurityCenter, o SecurityCenter fará o download e a instalação das atualizações automaticamente.

Fazer o download de atualizações automaticamente

Se você selecionar **Fazer o download das atualizações automaticamente e notificar-me quando estiverem prontas para ser instaladas** em Opções de atualização, o SecurityCenter fará o download das atualizações automaticamente e irá notificá-lo quando estiverem prontas para ser instaladas. Você pode optar por instalar ou adiar a atualização (página 30).

Para instalar uma atualização obtida por download automaticamente:

1. Clique em **Atualizar meus produtos agora** no alerta e clique em **OK**.

   Se solicitado, você deverá efetuar logon no site da Web para que sua assinatura seja verificada, antes de fazer o download.

2. Depois de verificar a assinatura, clique em **Atualizar** no painel Atualizações para fazer o download e instalar a atualização. Se a assinatura tiver expirado, clique em **Renovar minha assinatura** no alerta e siga as instruções.

Observação: Em alguns casos, você será solicitado a reiniciar o computador para concluir a atualização. Salve todo o seu trabalho e feche todos os programas antes de reiniciar.

Notificar antes de fazer o download das atualizações

Se você selecionar **Notificar-me antes de fazer o download de atualizações** no painel Opções de atualização, o SecurityCenter irá notificá-lo antes de fazer o download de qualquer atualização. Você pode optar por fazer o download e a instalação de uma atualização nos serviços de segurança para eliminar uma ameaça de ataque.

Para fazer o download e a instalação de uma atualização:

1. Selecione **Atualizar meus produtos agora** no alerta e clique em **OK**.

2. Se solicitado, efetue logon no site da Web.

   O download de atualização é feito automaticamente.

3. Clique em **OK** no alerta quando a instalação da atualização estiver concluída.

Observação: Em alguns casos, você será solicitado a reiniciar o computador para concluir a atualização. Salve todo o seu trabalho e feche todos os programas antes de reiniciar.

Desativar a atualização automática

Para obter proteção máxima, a McAfee recomenda que você deixe o SecurityCenter verificar e instalar as atualizações automaticamente. Entretanto, se desejar atualizar apenas manualmente os serviços de segurança, você poderá desativar a atualização automática.

> **Observação:** Você deve lembrar-se de verificar as atualizações manualmente (página 31) pelo menos uma vez por semana. Se você não verificar se há atualizações, seu computador não estará protegido pelas atualizações de segurança mais recentes .

Para desativar a atualização automática:

1. Em **Informações do SecurityCenter**, clique em **Configurar**.
2. Clique na seta ao lado do status de **Atualizações automáticas ativadas** para expandir o painel.
3. Clique em **Desligado**.
4. Clique em **Sim** para confirmar a alteração.

   O status é atualizado no cabeçalho.

Se você não verificar as atualizações manualmente em sete dias, é emitido um alerta para lembrá-lo.

Adiar atualizações

Se você não puder atualizar os serviços de segurança quando o alerta for exibido, poderá optar por ser lembrado posteriormente ou ignorar o alerta.

Para adiar uma atualização:

- Escolha uma das seguintes opções:
  - Selecione **Lembre-me mais tarde** no alerta e clique em **OK**.
  - Selecione **Fechar este alerta** e clique em **OK** para fechar o alerta sem executar nenhuma ação.

Verificar atualizações manualmente

O SecurityCenter verifica automaticamente se há atualizações a cada quatro horas quando você está conectado à Internet e, em seguida, instala as atualizações mais recentes do produto. Porém, você pode verificar atualizações manualmente a qualquer momento, usando o ícone do SecurityCenter na área de notificação do Windows, na extrema direita da barra de tarefas.

Observação: Para obter proteção máxima, a McAfee recomenda que você deixe o SecurityCenter verificar e instalar as atualizações automaticamente. Entretanto, se desejar atualizar apenas manualmente os serviços de segurança, você poderá desativar a atualização automática (página 30).

Para verificar manualmente se existem atualizações:

1. Verifique se o computador está conectado à Internet.
2. Clique com o botão direito no ícone M do SecurityCenter na área de notificação do Windows, na extrema direita da barra de tarefas e clique em **Atualizações**.

   Enquanto o SecurityCenter está verificando as atualizações, você continuar a executar outras tarefas com ele.

   Para maior praticidade, um ícone animado é exibido na área de notificação do Windows, na extrema direita da barra de tarefas. Quando o SecurityCenter tiver terminado, o ícone desaparecerá automaticamente.
3. Se solicitado, efetue logon no site da Web para que sua assinatura seja verificada.

Observação: Em alguns casos, você será solicitado a reiniciar o computador para concluir a atualização. Salve todo o seu trabalho e feche todos os programas antes de reiniciar.

Configurando opções de alerta

O SecurityCenter notifica automaticamente, por meio de alertas e sons, sobre epidemias públicas de vírus, ameaças à segurança e atualizações do produto. Porém, você pode configurar o SecurityCenter para mostrar somente alertas que exijam atenção imediata.

Configurar opções de alerta

O SecurityCenter notifica automaticamente, por meio de alertas e sons, sobre epidemias públicas de vírus, ameaças à segurança e atualizações do produto. Porém, você pode configurar o SecurityCenter para mostrar somente alertas que exijam atenção imediata.

Para configurar as opções de alerta:

1 Em **Informações do SecurityCenter**, clique em **Configurar**.

2 Clique na seta ao lado de **Alertas** para expandir o painel e clique em **Avançado**.

3 Selecione uma das opções a seguir no painel Opções de alerta:

- **Alertar-me quando ocorrer um surto público de um vírus ou uma ameaça à segurança**
- **Mostrar alertas informativos quando o modo de jogos for detectado**
- **Executar um som quando ocorrer um alerta**
- **Mostrar tela de abertura da McAfee ao iniciar o Windows**

4 Clique em **OK**.

Observação: Para desativar alertas informativos futuros a partir do próprio alerta, selecione a caixa **Não mostrar este alerta novamente**. Você pode ativá-lo novamente mais tarde no painel Alertas informativos.

Configurar alertas informativos

Os alertas informativos avisam você quando ocorrem eventos que não exigem resposta imediata. Se você desativar alertas informativos futuros a partir do próprio alerta, você poderá ativá-los novamente mais tarde no painel Alertas informativos.

Para configurar alertas informativos:

1. Em **Informações do SecurityCenter**, clique em **Configurar**.
2. Clique na seta ao lado de **Alertas** para expandir o painel e clique em **Avançado**.
3. Em **Configuração do SecurityCenter**, clique em **Alertas informativos**.
4. Desmarque a caixa de seleção **Ocultar alertas informativos** e, em seguida, desmarque as caixas de seleção dos alertas da lista que você deseja mostrar.
5. Clique em **OK**.

CAPÍTULO 5

Executando tarefas comuns

Você pode executar tarefas comuns, incluindo retornar ao painel Início, exibir eventos recentes, gerenciar a rede do computador (se for um computador com recursos de gerenciamento para esta rede) e manutenção do computador. Se o McAfee Data Backup estiver instalado, você também poderá fazer backup de dados.

Neste capítulo

Executar tarefas comuns

Você pode executar tarefas comuns, incluindo retornar ao painel Início, exibir eventos recentes, fazer a manutenção do computador, gerenciar a rede (se for um computador com recursos de gerenciamento para esta rede), além de fazer backup de dados (se o McAfee Data Backup estiver instalado).

Para executar tarefas comuns:

- Em **Tarefas comuns** no Menu básico, execute um dos procedimentos a seguir:
  - Para retornar ao painel Início, clique em **Início**.
  - Para exibir eventos recentes detectados por seu software de segurança, clique em **Eventos recentes**.
  - Para remover arquivos não utilizados, desfragmentar dados e restaurar as configurações anteriores do computador, clique em **Manter o computador**.
  - Para gerenciar a rede do computador, clique em **Gerenciar rede**, em um computador com recurso de gerenciamento para esta rede.

    O Network Manager monitora as falhas de segurança dos computadores em sua rede para que você possa identificar problemas de segurança de rede facilmente.
  - Para criar cópias de backup de seus arquivos, clique em **Data Backup**, se o McAfee Data Backup estiver instalado.

O backup automático salva cópias de seus arquivos mais valiosos onde você desejar, criptografando e armazenando os arquivos em um CD/DVD, em uma unidade USB, externa ou de rede.

Dica: Para maior praticidade, você pode realizar tarefas comuns a partir de dois outros locais (em **Início**, no Menu avançado, e no menu **QuickLinks** do ícone M do SecurityCenter, na extrema direita da barra de tarefas). Também é possível exibir eventos recentes e registros abrangentes por tipo em **Relatórios e registros**, no Menu avançado.

Exibir eventos recentes

Eventos recentes são registrados quando ocorrem alterações no computador. Isso ocorre, por exemplo, quando um tipo de proteção é ativado ou desativado, quando uma ameaça é removida ou quando a tentativa de conexão com a Internet é bloqueada. Você pode exibir os 20 eventos mais recentes e seus detalhes.

Consulte o arquivo da Ajuda do produto em questão para obter detalhes sobre seus eventos.

Para exibir eventos recentes:

1. Clique com o botão direito no ícone do SecurityCenter, aponte para **QuickLinks**, e clique em **Exibir eventos recentes**.

   Todos os eventos recentes aparecerão na lista, mostrando a data e uma descrição breve.

2. Em **Eventos recentes**, selecione um evento para exibir informações adicionais no painel Detalhes.

   Em **Desejo**, serão exibidas as ações disponíveis.

3. Para exibir uma lista mais abrangente de eventos, clique em **Exibir registro**.

Fazer a manutenção do computador automaticamente

Para liberar um espaço valioso na unidade e otimizar o desempenho do computador, você pode programar as tarefas QuickClean ou Desfragmentador de disco para que sejam executadas em intervalos regulares. Essas tarefas incluem exclusão, destruição e desfragmentação de arquivos e pastas.

Para fazer a manutenção do computador automaticamente:

1. Clique com o botão direito no ícone do SecurityCenter, aponte para **QuickLinks**, em seguida, clique em **Manter o computador**.
2. Em **Programador de tarefas**, clique em **Iniciar**.
3. Na lista de operação, selecione **QuickClean** ou **Desfragmentador de disco**.
4. Escolha uma das seguintes opções:
   - Para modificar uma tarefa existente, selecione-a e clique em **Modificar**. Siga as instruções da tela.
   - Para criar uma nova tarefa, digite o nome na caixa **Nome da tarefa** e clique em **Criar**. Siga as instruções da tela.
   - Para excluir uma tarefa, selecione-a e clique em **Excluir**.
5. Em **Resumo da tarefa**, veja quando a tarefa foi executada pela última vez, quando será executada novamente e seu status.

Fazer a manutenção do computador manualmente

Você pode executar tarefas manuais de manutenção para remover arquivos não utilizados, desfragmentar seus dados ou restaurar as configurações anteriores do computador.

Para fazer a manutenção do computador manualmente:

- Escolha uma das seguintes opções:
  - Para usar o QuickClean, clique com o botão direito no ícone do SecurityCenter, aponte para **QuickLinks**, clique em **Manter o computador** e, em seguida, clique em **Iniciar**.
  - Para usar o Desfragmentador de disco, clique com o botão direito no ícone do SecurityCenter, aponte para **QuickLinks**, clique em **Manter o computador**.e, em seguida, clique em **Analisar**.
  - Para usar a Restauração de sistema , no Menu avançado, clique em **Ferramentas**, **Restauração do sistema** e, em seguida, clique em **Iniciar**.

Remover arquivos e pastas não utilizados

Use o QuickClean para liberar um espaço valioso na unidade e otimizar o desempenho do computador.

Para remover arquivos e pastas não utilizados:

1. Clique com o botão direito no ícone do SecurityCenter, aponte para **QuickLinks**, em seguida, clique em **Manter o computador**.
2. Em **QuickClean**, clique em **Iniciar**.
3. Siga as instruções da tela.

Desfragmentar arquivos e pastas

A fragmentação de arquivos ocorre quando arquivos e pastas são excluídos e novos arquivos são adicionados. Essa fragmentação torna o acesso ao disco mais lento e prejudica o desempenho geral do computador, embora não de forma grave, normalmente.

Use a desfragmentação para regravar partes de um arquivo para setores contíguos em um disco rígido, de modo a aumentar a velocidade de acesso e recuperação.

Para desfragmentar arquivos e pastas:

1 Clique com o botão direito no ícone do SecurityCenter, aponte para **QuickLinks**, e clique em **Manter o computador**.

2 Em **Desfragmentador de disco**, clique em **Analisar**.

3 Siga as instruções da tela.

Restaurar as configurações anteriores do computador

Pontos de restauração são instantâneos do computador que o Windows salva periodicamente e quando ocorrem eventos significativos (como a instalação de um programa ou unidade). Porém, você pode criar e nomear seus próprios pontos de restauração a qualquer momento.

Use pontos de restauração para desfazer alterações nocivas no computador e retornar às configurações anteriores.

Para restaurar as configurações anteriores do computador:

1 No Menu avançado, clique em **Ferramentas** e clique em **Restauração do sistema**.

2 Em **Restauração do sistema**, clique em **Iniciar**.

3 Siga as instruções da tela.

Gerenciar a rede

Se o computador tiver recursos de gerenciamento para sua rede, você poderá usar o Network Manager para monitorar computadores em toda a rede para identificar problemas de segurança de rede facilmente.

Se o status de proteção do computador não estiver sendo monitorado nesta rede, então o computador não pertence à rede ou é um membro não gerenciado da rede. Consulte detalhes no arquivo da Ajuda do Network Manager.

Para gerenciar sua rede:

1. Clique com o botão direito no ícone do SecurityCenter, aponte para **QuickLinks** e clique em **Gerenciar rede**.
2. Clique no ícone que representa este computador no mapa da rede.
3. Em **Desejo**, clique em **Monitorar este computador**.

Saiba mais sobre vírus

Use a Biblioteca de informações sobre vírus e o Virus Map e:

- Saiba mais sobre os mais recentes vírus, embustes de vírus em e-mail e outras ameaças.
- Obtenha ferramentas gratuitas de remoção de vírus para ajudar a reparar seu computador.
- Obtenha uma visão geral em tempo real dos locais em que os vírus mais recentes estão infectando computadores no mundo todo.

Para saber mais sobre vírus:

1. No Menu avançado, clique em **Ferramentas** e clique em **Informações sobre vírus**.
2. Escolha uma das seguintes opções:
   - Pesquise vírus usando a Biblioteca de informações sobre vírus gratuita da McAfee.
   - Pesquise vírus usando o World Virus Map no site da McAfee na Web.

CAPÍTULO 6

McAfee QuickClean

Resíduos se acumulam rapidamente em seu computador ao navegar na Internet. Com o QuickClean, você protege a sua privacidade e exclui os resíduos de Internet e de e-mail que não são necessários. O QuickClean identifica e exclui os arquivos que se acumulam durante a navegação, incluindo cookies, e-mails, downloads e históricos—dados que contêm informações pessoais sobre você. Ele protege a sua privacidade, oferecendo exclusão segura destas informações confidenciais.

O QuickClean também exclui programas indesejados. Especifique os arquivos que você deseja eliminar e livre-se dos resíduos sem excluir as informações essenciais.

Neste capítulo

Noções básicas sobre os recursos do QuickClean

Esta seção descreve os recursos do QuickClean.

Recursos

O QuickClean fornece um conjunto de ferramentas eficientes e de fácil utilização que exclui com segurança os fragmentos digitais. Você pode liberar um valioso espaço na unidade e otimizar o desempenho do seu computador.

CAPÍTULO 7

Limpando o computador

O QuickClean permite excluir com segurança os arquivos e as pastas.

Ao navegar na Internet, seu navegador copia cada página da Internet e seus gráficos para uma pasta em cache em seu disco. O navegador então pode carregar a página rapidamente, se você voltar a visitá-la. Armazenar os arquivos em cache é útil se você visita várias vezes as mesmas páginas da Internet e se os conteúdos das páginas não são alterados com freqüência. No entanto, na maioria das vezes, os arquivos em cache não são úteis e podem ser excluídos.

Você pode excluir diversos itens com os seguintes limpadores.

- Limpador da lixeira: Limpa a sua lixeira do Windows.
- Limpador de arquivos temporários: Exclui os arquivos armazenados nas pastas temporárias.
- Limpador de atalhos: Exclui os atalhos quebrados e os atalhos sem um programa associado.
- Limpador de fragmentos perdidos de arquivos: Exclui os fragmentos de arquivos perdidos de seu computador.
- Limpador de registro: Exclui as informações do Registro do Windows para programas que não existem mais em seu computador.
- Limpador de cache: Exclui os arquivos em cache que se acumulam quando você navega na Internet. Arquivos desse tipo normalmente são armazenados como arquivos temporários da Internet.
- Limpador de cookies: Exclui os cookies. Arquivos desse tipo normalmente são armazenados como arquivos temporários da Internet.
  Os cookies são arquivos pequenos que o navegador da Web armazena no computador atendendo a uma solicitação do servidor Web. Toda vez que você exibir uma página da Web do servidor Web, o navegador enviará o cookie de volta ao servidor. Esses cookies podem agir como uma marca, permitindo que o servidor Web rastreie as páginas que foram exibidas e a freqüência na qual você volta nelas.
- Limpador de histórico do navegador: Exclui seu histórico de navegador.
- Limpador de e-mails do Outlook Express e do Outlook para itens excluídos e enviados: Exclui o correio das pastas Enviadas e Excluídas do Outlook.

- Limpador usado recentemente: Exclui os itens usados recentemente e armazenados em seu computador, como documentos do Microsoft Office.
- Limpador de ActiveX e de plug-in: Exclui controles e plug-ins do ActiveX.
  O ActiveX é uma tecnologia usada para implementar os controles em um programa. Um controle ActiveX pode adicionar um botão à interface de um programa. A maioria desses controles são inofensivos; no entanto, algumas pessoas podem usar a tecnologia ActiveX para capturar as informações de seu computador.
  Os plug-ins são pequenos programas de software que se conectam a aplicativos maiores para fornecer funcionalidade adicional. Plug-ins permitem que o navegador da Web acesse e execute os arquivos incorporados nos documentos HTML que estejam em formatos que o navegador normalmente não reconheceria (por exemplo, animação, vídeo e arquivos de áudio).
- Limpador do ponto de restauração do sistema: Exclui os antigos pontos de restauração do sistema do seu computador.

Neste capítulo

Usando o QuickClean

Esta seção descreve como utilizar o QuickClean.

Limpe o seu computador

Você pode excluir arquivos e pastas não usados, liberar espaço em disco e permitir que seu computador seja executado com mais eficiência.

Para limpar o seu computador:

1. No menu Avançado, clique em **Ferramentas**.
2. Clique em **Manter o computador** e, em seguida, clique em **Iniciar** em **McAfee QuickClean**.
3. Escolha uma das seguintes opções:
   - Clique em **Avançar** para aceitar os limpadores padrão na lista.
   - Selecione ou desmarque os limpadores apropriados e, em seguida, clique em **Avançar.** Para o Limpador usado recentemente, você pode clicar em **Propriedades** para desmarcar os programas cujas listas você não deseja limpar.
   - Clique em **Restaurar padrões** para restaurar os limpadores padrão e, em seguida, clique em **Avançar.**
4. Depois que a análise for executada, clique em **Avançar** para confirmar a exclusão do arquivo. Você pode expadir essa lista para ver os arquivos que serão limpos e seus locais.
5. Clique em **Avançar.**
6. Escolha uma das seguintes opções:
   - Clique em **Avançar** para aceitar o padrão **Não, desejo excluir os arquivos usando a exclusão padrão do Windows**.
   - Clique em **Sim, desejo apagar com segurança os meus arquivos usando o Shredder** e especificar o número de etapas. Arquivos excluídos com o Shredder não podem ser recuperados.
7. Clique em **Concluir**.
8. Em **Resumo do QuickClean**, exiba o número de arquivos de Registro que foram excluídos e a quantidade de espaço em disco recuperada após a limpeza do disco e da Internet.

CAPÍTULO 8

McAfee Shredder

Os arquivos excluídos podem ser recuperados no seu computador até mesmo depois do esvaziamento da Lixeira. Quando um arquivo é excluído, o Windows marca esse espaço na unidade de disco para indicar que ele não está mais sendo utilizado, mas o arquivo continua presente. Usando ferramentas de análise legal do computador, você pode recuperar registros de impostos, currículos ou outros documentos que tenham sido excluídos. O Shredder protege a sua privacidade, excluindo os arquivos indesejados de forma segura e permanente.

Para excluir um arquivo permanentemente, é preciso sobrescrever várias vezes o arquivo existente com novos dados. O Microsoft® Windows não exclui os arquivos com segurança, porque cada operação de arquivo seria muito lenta. A destruição de um documento nem sempre impede que ele seja recuperado, pois alguns programas fazem cópias ocultas temporárias de documentos abertos. Se você destruiu apenas os documentos exibidos no Windows® Explorer, ainda pode haver cópias temporárias desses documentos.

Observação: Não é feito o backup dos arquivos destruídos. Você não pode restaurar os arquivos que o Shredder excluiu.

Neste capítulo

Noções básicas dos recursos do Shredder

Esta seção descreve os recursos do Shredder.

Recursos

O Shredder permite apagar o conteúdo da Lixeira, os arquivos temporários da Internet, o histórico do site da Web, os arquivos, as pastas e os discos.

CAPÍTULO 9

Apagando arquivos indesejados com o Shredder

O Shredder protege a sua privacidade, excluindo de forma segura e permanente os arquivos indesejados, como o conteúdo da Lixeira, os arquivos temporários da Internet e o histórico do site da Web. Você pode selecionar os arquivos e as pastas a serem destruídos ou procurar por eles.

Neste capítulo

Usando o Shredder

Esta seção descreve como utilizar o Shredder.

Arquivos, pastas e discos destruídos

Os arquivos podem permanecer em seu computador mesmo depois que você esvaziar a sua Lixeira. No entanto, ao destruir os arquivos, os seus dados são permanentemente excluídos e os hackers não podem acessá-los.

Para destruir arquivos, pastas e discos:

1. No menu Avançado, clique em **Ferramentas** e, em seguida, clique em **Shredder**.
2. Escolha uma das seguintes opções:
   - Clique em **Apagar arquivos e pastas** para destruir os arquivos e as pastas.
   - Clique em **Apagar um disco inteiro** para destruir discos**.**
3. Selecione um dos seguintes níveis de destruição:
   - **Rápida**: Destrói os itens selecionados em uma única etapa.
   - **Abrangente**: Destrói os itens selecionados em sete etapas.
   - **Personalizada**: Destrói os itens selecionados em até dez etapas. Um número superior de etapas de destruição aumenta o nível de exclusão do arquivo de segurança.
4. Clique em **Avançar**.
5. Escolha uma das seguintes opções:
   - Se você estiver destruindo arquivos, clique em **Conteúdo da Lixeira**, **Arquivos temporários da Internet** ou **Histórico do site da Web** na lista **Selecionar arquivos a serem destruídos**. Se você estiver destruindo um disco, clique no disco.
   - Clique em **Procurar**, navegue até os arquivos que você deseja destruir e, em seguida, selecione-os.
   - Digite o caminho até os arquivos que você deseja destruir na lista **Selecionar arquivos a serem destruídos**.
6. Clique em **Avançar**.
7. Clique em **Concluir** para concluir a operação.
8. Clique em **Concluído.**

CAPÍTULO 10

McAfee Network Manager

O McAfee® Network Manager apresenta uma exibição gráfica dos computadores e componentes que fazem parte da sua rede doméstica. Você pode usar o Network Manager para monitorar remotamente o status de proteção de cada computador gerenciado da sua rede e para corrigir remotamente as vulnerabilidades de segurança reportadas nesses computadores gerenciados.

Antes de começar a usar o Network Manager, você pode se familiarizar com alguns dos recursos mais populares. A Ajuda do Network Manager fornece detalhes sobre como configurar e usar esses recursos.

Neste capítulo

Recursos

O Network Manager oferece os seguintes recursos:

Mapa gráfico da rede

O mapa de rede do Network Manager oferece uma representação gráfica do status de segurança dos computadores e componentes que fazem parte de sua rede doméstica. Quando você faz modificações na rede (adicionando um computador, por exemplo), o mapa de rede reconhece essas alterações. Você pode atualizar o mapa de rede, renomear a rede e mostrar ou ocultar componentes do mapa de rede, para personalizar sua exibição. Também é possível exibir os detalhes associados a qualquer dos componentes exibidos no mapa de rede.

Gerenciamento remoto

Use o mapa de rede do Network Manager para gerenciar o status de segurança dos computadores que fazem parte de sua rede doméstica. Você pode convidar um computador a associar-se à rede gerenciada, monitorar o status de segurança dos computadores gerenciados e corrigir vulnerabilidades de segurança conhecidas a partir de um computador remoto da rede.

Noções básicas sobre os ícones do Network Manager

A tabela a seguir descreve os ícones geralmente usados no mapa de rede do Network Manager.

Ícone	Descrição
	Representa um computador gerenciado on-line
	Representa um computador gerenciado off-line
	Representa um computador não gerenciado com o software de segurança McAfee 2007 instalado
	Representa um computador não gerenciado off-line
	Representa um computador on-line sem o software de segurança McAfee 2007 instalado ou um dispositivo de rede desconhecido
	Representa um computador off-line sem o software de segurança McAfee 2007 instalado ou um dispositivo de rede desconhecido off-line
	Significa que o item correspondente está protegido e conectado
	Significa que o item correspondente exige a sua atenção
	Significa que o item correspondente exige a sua atenção e está desconectado
	Representa um roteador doméstico sem fio
	Representa um roteador doméstico padrão
	Representa a Internet, quando conectada
	Representa a Internet, quando desconectada

CAPÍTULO 11

Configurando uma rede gerenciada

Você configura uma rede gerenciada trabalhando com os itens de seu mapa de rede e adicionando membros (computadores) a ela.

Neste capítulo

Trabalhando com o mapa de rede

Sempre que um computador é conectado à rede, o Network Manager analisa o estado da rede para determinar a presença de membros (gerenciados ou não), os atributos do roteador e o status da Internet. Se nenhum membro for encontrado, o Network Manager presume que o computador conectado atualmente é o primeiro computador da rede e automaticamente o torna um membro gerenciado com permissões administrativas. Por padrão, o nome da rede inclui o grupo de trabalho ou o domínio do primeiro computador conectado à rede com o software de segurança McAfee 2007 instalado. Contudo, você pode renomear a rede a qualquer momento.

Quando fizer modificações na rede (adicionando um computador, por exemplo), você poderá personalizar o mapa de rede. Por exemplo, você pode atualizar o mapa de rede, renomear a rede e mostrar ou ocultar componentes do mapa de rede, para personalizar sua exibição. Também é possível exibir os detalhes associados a qualquer dos componentes exibidos no mapa de rede.

Acessar o mapa de rede

Para acessar um mapa da sua rede, inicie o Network Manager a partir da lista de tarefas comuns do SecurityCenter. O mapa de rede fornece uma representação gráfica dos computadores e componentes que fazem parte da sua rede doméstica.

Para acessar o mapa de rede:

- No menu Básico ou Avançado, clique em **Gerenciar rede**.
  O mapa de rede é exibido no painel direito.

Observação: Quando acessar o mapa de rede pela primeira vez, você será solicitado a confiar nos outros computadores da rede antes que o mapa de rede seja exibido.

Atualizar o mapa de rede

Você pode atualizar o mapa da rede a qualquer momento; por exemplo, depois que outro computador associa-se à rede gerenciada.

Para atualizar o mapa de rede:

1. No menu Básico ou Avançado, clique em **Gerenciar rede**.
   O mapa de rede é exibido no painel direito.
2. Clique em **Atualizar o mapa de rede**, em **Desejo**.

Observação: O link **Atualizar o mapa de rede** só está disponível quando não há itens selecionados no mapa de rede. Para desmarcar um item, clique no item selecionado ou clique em uma área em branco no mapa de rede.

Renomear a rede

Por padrão, o nome da rede inclui o nome do grupo de trabalho ou do domínio do primeiro computador conectado à rede com software de segurança McAfee 2007 instalado. Se esse nome não for adequado, você poderá mudá-lo.

Para renomear a rede:

1. No menu Básico ou Avançado, clique em **Gerenciar rede**.
   O mapa de rede é exibido no painel direito.
2. Clique em **Renomear a rede**, em **Desejo**.
3. Digite o nome da rede na caixa **Renomear rede**.
4. Clique em **OK**.

Observação: O link **Renomear rede** só está disponível quando não há itens selecionados no mapa de rede. Para desmarcar um item, clique no item selecionado ou clique em uma área em branco no mapa de rede.

Mostrar ou ocultar itens do mapa de rede

Por padrão, todos os computadores e componentes da sua rede doméstica são exibidos no mapa de rede. Contudo, se você tiver ocultado itens, é possível exibi-los novamente a qualquer momento. Somente os itens não gerenciados podem ser ocultados; não é possível ocultar os computadores gerenciados.

Para...	No menu Básico ou Avançado, clique em **Gerenciar rede** e, em seguida realize este procedimento...
Ocultar um item no mapa de rede	Clique em um item do mapa de rede e clique em **Ocultar este item** em **Desejo**. Na caixa de diálogo de confirmação, clique em **Sim**.
Mostrar itens ocultos no mapa de rede	Em **Desejo**, clique em **Mostrar itens ocultos**.

Exibir detalhes do item

Você pode exibir as informações detalhadas de qualquer componente da sua rede, selecionando-o no mapa de rede. Essas informações incluem o nome do componente, seu status de proteção e outros dados necessários para gerenciá-lo.

Para exibir os detalhes de um item:

1. Clique no ícone de um item no mapa de rede.
2. Em **Detalhes**, exiba as informações sobre o item.

Associando à rede gerenciada

Para que um computador possa ser gerenciado remotamente ou receber permissão para gerenciar outros computadores remotamente, ele deve se tornar um membro confiável da rede. A associação à rede é concedida para novos computadores por membros existentes da rede (computadores) com permissões administrativas. Para garantir que apenas computadores confiáveis se associem à rede, os usuários do computador que concede a permissão e do computador que está se associando a ela devem autenticar um ao outro.

Quando um computador se associa à rede, ele é solicitado a mostrar o seu status de proteção do McAfee para outros computadores da rede. Se um computador concordar em mostrar seu status de proteção, ele se tornará um membro *gerenciado* da rede. Se um computador se recusar a mostrar seu status de proteção, ele se tornará um membro *não gerenciado* da rede. Os membros não gerenciados da rede geralmente são computadores convidados que desejam acesso a outros recursos de rede (como, por exemplo, compartilhamento de arquivos ou da impressora).

Observação: Depois da associação, se você tiver outros programas de rede da McAfee instalados (o McAfee Wireless Network Security ou o EasyNetwork, por exemplo), o computador também será reconhecido como membro gerenciado nesses programas. O nível de permissão atribuído a um computador no Network Manager aplica-se a todos os programas de rede da McAfee. Para obter mais informações sobre o que significam permissões de convidado, total ou administrativa em outros programas de rede da McAfee, consulte a documentação fornecida com o programa.

Associar-se a uma rede gerenciada

Quando receber um convite para se associar a uma rede gerenciada, você poderá aceitar ou rejeitar o convite. Também é possível determinar se deseja que este computador e os outros computadores da rede monitorem as configurações de segurança uns dos outros (se os serviços de proteção contra vírus estão atualizados ou não, por exemplo).

Para associar-se a uma rede gerenciada:

1. Na caixa de diálogo de convite, marque a caixa de seleção **Permitir que este computador e outros computadores monitorem as configurações de segurança uns dos outros** para permitir que outros computadores da rede gerenciada monitorem as configurações de segurança do seu computador.
2. Clique em **Associar-se**.
   Quando você aceitar o convite, duas cartas de baralho serão exibidas.
3. Confirme se as cartas de baralho são as mesmas exibidas no computador que o convidou para se associar à rede gerenciada.
4. Clique em **Confirmar**.

Observação: Se o computador que o convidou não exibir as mesmas cartas que estão sendo exibidas na caixa de diálogo de confirmação de segurança, isso significa que houve uma violação de segurança na rede gerenciada. Associar-se à rede poderia colocar seu computador em risco, portanto, clique em **Rejeitar** na caixa de diálogo de confirmação de segurança.

Convidar um computador para associar-se à rede gerenciada

Se um computador for adicionado ou outro computador não gerenciado estiver presente na rede, você poderá convidá-lo a se associar à rede gerenciada. Apenas os computadores com permissões administrativas na rede podem convidar outros computadores. Ao enviar um convite, você também poderá especificar o nível de permissão que deseja atribuir ao computador que irá se associar.

Para convidar um computador para associar-se à rede gerenciada:

1. Clique no ícone de um computador não gerenciado no mapa de rede.
2. Clique em **Monitorar este computador**, em **Desejo.**
3. Na caixa de diálogo Convidar um computador para associar-se a esta rede gerenciada, clique em uma destas opções:
   - **Conceder acesso convidado**
     O acesso de convidado permite que o computador acesse a rede.
   - **Conceder acesso total para todos os aplicativos da rede gerenciada**
     O acesso total (como o acesso de convidado) permite que o computador acesse a rede.
   - **Conceder acesso administrativo para todos os aplicativos da rede gerenciada**
     O acesso administrativo permite que o computador acesse a rede com permissões administrativas. Ele também permite que o computador conceda acesso a outros computadores que queiram se associar à rede gerenciada.

4 Clique em **Convidar**.
Um convite para se associar à rede gerenciada é enviado para o computador. Quando o computador aceitar o convite, duas cartas de baralho são exibidas.

5 Confirme se as cartas de baralho são as mesmas exibidas no computador que você convidou para se associar à rede gerenciada.

6 Clique em **Conceder acesso**.

Observação: Se o computador que você convidou não exibir as mesmas cartas que estão sendo exibidas na caixa de diálogo de confirmação de segurança, isso significa que houve uma violação de segurança na rede gerenciada. Permitir que o computador tenha acesso à rede pode colocar outros computadores em risco, portanto, clique em **Rejeitar acesso** na caixa de diálogo de confirmação de segurança.

Parar de confiar nos computadores da rede

Caso tenha concordado em confiar em outros computadores por engano, você pode parar de confiar neles.

Para parar de confiar nos computadores da rede:

- Clique em **Parar de confiar nos computadores desta rede** em **Desejo**.

Observação: O link **Parar de confiar nos computadores desta rede** só estará disponível quando nenhum outro computador gerenciado tiver se associado à rede.

CAPÍTULO 12

Gerenciando a rede remotamente

Depois de configurar sua rede gerenciada, você pode usar o Network Manager para gerenciar remotamente os computadores e componentes que fazem parte da rede. É possível gerenciar o status e os níveis de permissão dos computadores e componentes e corrigir vulnerabilidades da segurança remotamente.

Neste capítulo

Monitorando status e permissões

Uma rede gerenciada possui dois tipos de membros: membros gerenciados e não gerenciados. Membros gerenciados permitem que outros computadores da rede monitores seu status de proteção McAfee, enquanto membros não gerenciados não o permitem. Os membros não gerenciados geralmente são computadores convidados que desejam acessar outros recursos da rede (como, por exemplo, compartilhamento de arquivos ou de impressora). Um computador não gerenciado pode ser convidado a se tornar gerenciado a qualquer momento por outro computador da rede. Da mesma forma, um computador danificado pode se tornar não gerenciado a qualquer momento.

Os computadores gerenciados possuem uma permissão administrativa, total ou de convidado. As permissões administrativas permitem que o computador gerenciado gerencie o status de proteção de todos os computadores gerenciados na rede e que conceda acesso à rede para outros computadores. As permissões total e de convidado permitem somente que um computador acesse a rede. Você pode modificar o nível de permissão de um computador a qualquer momento.

Como uma rede gerenciada também é composta por dispositivos (como roteadores, por exemplo), você poderá usar o Network Manager para gerenciá-los. Também é possível configurar e modificar as propriedades de exibição do dispositivo no mapa de rede.

Monitorar o status de proteção de um computador

Se o status de proteção de um computador não estiver sendo monitorado na rede (porque o computador não é um membro da rede ou não é gerenciado), você pode fazer uma solicitação para monitorá-lo.

Para monitorar o status de proteção de um computador:

1. Clique no ícone de um computador não gerenciado no mapa de rede.
2. Clique em **Monitorar este computador**, em **Desejo**.

Parar de monitorar o status de proteção de um computador

Você pode parar de monitorar o status de proteção de um computador gerenciado em sua rede particular. A partir desse momento o computador não será mais gerenciado.

Para parar de monitorar o status de proteção de um computador:

1. Clique no ícone de um computador gerenciado no mapa de rede.
2. Clique em **Parar de monitorar este computador**, em **Desejo**.
3. Na caixa de diálogo de confirmação, clique em **Sim**.

Modificar as permissões de um computador gerenciado

Você pode modificar as permissões de um computador gerenciado a qualquer momento. Isso permite que você ajuste os computadores que poderão monitorar os status de proteção (configurações de segurança) de outros computadores da rede.

Para modificar as permissões de um computador gerenciado:

1. Clique no ícone de um computador gerenciado no mapa de rede.
2. Clique em **Monitorar permissões para este computador**, em **Desejo**.
3. Na caixa de diálogo de modificação das permissões, marque ou desmarque a caixa de seleção que determina se este e outros computadores da rede gerenciada poderão monitorar o status de proteção uns dos outros.
4. Clique em **OK**.

Gerenciar um dispositivo

Você pode gerenciar um dispositivo acessando a sua página administrativa da Web a partir do Network Manager.

Para gerenciar um dispositivo:

1 Clique no ícone de um dispositivo no mapa de rede.

2 Clique em **Gerenciar este dispositivo**, em **Desejo**.
Um navegador da Web é aberto e exibe a página administrativa do dispositivo na Web.

3 No navegador da Web, insira as suas informações de logon e defina as configurações de segurança do dispositivo.

Observação: Se o dispositivo for um ponto de acesso ou um roteador sem fio protegido pelo Wireless Network Security, você terá que usar o Wireless Network Security para definir as configurações de segurança do dispositivo.

Modificar as propriedades de exibição de um dispositivo

Ao modificar as propriedades de exibição de um dispositivo, você poderá alterar o nome de exibição do dispositivo no mapa da rede e especificar se ele é um roteador sem fio.

Para modificar as propriedades de exibição de um dispositivo:

1 Clique no ícone de um dispositivo no mapa de rede.

2 Clique em **Modificar propriedades de dispositivo**, em **Desejo**.

3 Para especificar o nome de exibição do dispositivo, digite um nome na caixa **Nome**.

4 Para especificar o tipo de dispositivo, clique em uma das seguintes opções:

- **Roteador**
Representa um roteador doméstico padrão.

- **Roteador sem fio**
Representa um roteador doméstico sem fio.

5 Clique em **OK**.

Corrigindo vulnerabilidades de segurança

Computadores gerenciados com permissões administrativas podem monitorar o status de proteção McAfee de outros computadores gerenciados na rede e corrigir remotamente quaisquer problemas de vulnerabilidade de segurança reportados. Por exemplo, se o status de proteção McAfee de um computador indicar que o VirusScan está desativado, outro computador gerenciado com permissões administrativas poderá *corrigir* essa vulnerabilidade de segurança, ativando o VirusScan remotamente.

Quando vulnerabilidades de segurança são corrigidas remotamente, o Network Manager automaticamente repara a maioria dos problemas reportados. No entanto, algumas vulnerabilidades podem exigir intervenção manual no computador local. Nesse caso, o Network Manager corrige os problemas que podem ser reparados remotamente e solicita que você corrija os problemas restantes efetuando login no SecurityCenter no computador vulnerável e seguindo as recomendações fornecidas. Em alguns casos, a correção sugerida é a instalação do software de segurança McAfee 2007 nos computadores remotos da rede.

Corrigir vulnerabilidades de segurança

Você pode usar o Network Manager para corrigir automaticamente a maioria das vulnerabilidades de segurança em computadores gerenciados remotos. Por exemplo, se o VirusScan estiver desativado em um computador remoto, você poderá usar o Network Manager para ativá-lo automaticamente.

Para corrigir vulnerabilidades de segurança:

1. Clique no ícone de um item no mapa de rede.
2. Exiba o status de proteção do item, em **Detalhes**.
3. Clique em **Corrigir vulnerabilidades de segurança**, em **Desejo**.
4. Depois de corrigir os problemas de segurança, clique em **OK**.

Observação: Apesar de o Network Manager corrigir automaticamente a maioria das vulnerabilidades de segurança, para efetuar alguns reparos pode ser necessário iniciar o SecurityCenter no computador vulnerável e seguir as recomendações fornecidas.

Instalar software de segurança McAfee em computadores remotos

Se um ou mais computadores de sua rede não estiverem executando software de segurança McAfee, o status de segurança deles não poderá ser monitorado remotamente. Se desejar monitorar esses computadores remotamente, você deverá ir até cada um deles e instalar o software de segurança McAfee.

Para instalar software de segurança McAfee em computadores remotos:

1 Em um navegador no computador remoto, vá para http://download.mcafee.com/us/.

2 Siga as instruções na tela para instalar o software de segurança Mcafee no computador.

C A P Í T U L O 1 3

McAfee Wireless Network Security

Através de uma interface fácil e intuitiva de apenas um clique, o Wireless Network Security oferece proteção automática padrão do setor contra roubo de dados, acesso não autorizado à rede e uso "clandestino" de banda larga. O Wireless Network Security criptografa os seus dados pessoais e privados à medida que estes são enviados por Wi-Fi e impede que hackers tenham acesso à sua rede sem fio.

O Wireless Network Security bloqueia o ataque de hackers à sua rede sem fio da seguinte forma:

- Impedindo que pessoas não autorizadas conectem-se à rede Wi-Fi
- Impedindo a captura de dados que são transmitidos através de uma rede Wi-Fi
- Detectando tentativas de conexão a uma rede Wi-Fi

O Wireless Network Security combina recursos com facilidade de uso, como o bloqueio instantâneo de rede e a rápida inclusão de usuários legítimos à rede, com recursos excelentes de segurança, como a criação automática de chave criptografada e rotação de chaves programada.

Neste capítulo

Recursos

O Wireless Network Security oferece os seguintes recursos:

Proteção sempre ativada

O Wireless Network Security detecta e protege automaticamente qualquer rede sem fio vulnerável à qual você se conecte.

Interface intuitiva

Protege sua rede sem a necessidade de tomar decisões difíceis ou conhecer termos técnicos complexos.

Criptografia automática forte

Permita que apenas os seus amigos e familiares tenham acesso à sua rede e proteja os seus dados durante o tráfego de informações.

Uma solução inteiramente em software

O Wireless Network Security trabalha com o seu software de segurança e o seu roteador ou ponto de acesso sem fio padrão. Não é necessário adquirir hardware adicional.

Rotação de chaves automática

Mesmo os hackers mais determinados não conseguem capturar as suas informações, pois a chave está sempre sendo alterada.

Acréscimo de usuários de rede

Você pode facilmente conceder acesso à sua rede para seus amigos e familiares. Você pode adicionar usuários pela rede sem fio ou pela transferência de software usando uma unidade USB.

Ferramenta de conexão intuitiva

A ferramenta de conexão sem fio é intuitiva e informativa, com detalhes sobre a intensidade do sinal e as condições de segurança.

Alertas e registro de eventos

Alertas e relatórios de fácil interpretação oferecem aos usuários avançados mais informações sobre a rede sem fio.

Modo de suspensão

Suspenda temporariamente a rotação de chaves para que determinados aplicativos possam funcionar sem interrupção.

Compatibilidade com outros equipamentos

O Wireless Network Security atualiza-se automaticamente com os mais recentes módulos de roteadores ou de pontos de acesso sem fio das marcas mais populares, como: Linksys®, NETGEAR®, D-Link®, Belkin®, TRENDnet® e outras.

Iniciando o Wireless Network Security

Após a instalação, o Wireless Network Security é ativado automaticamente; não é necessário iniciá-lo manualmente. Entretanto, você pode ativar e desativar manualmente a proteção sem fio.

Depois que você instalar o Wireless Network Security, seu computador tentará estabelecer uma conexão com o roteador sem fio. Após estabelecida a conexão, o computador programa a chave de criptografia dentro do roteador sem fio. Caso a senha padrão tenha sido alterada, será solicitada uma senha com a qual o Wireless Network Security possa configurar o roteador sem fio com a chave criptografada compartilhada e um modo de segurança forte. Seu computador também é configurado com a mesma chave compartilhada e o mesmo modo de criptografia, estabelecendo uma conexão sem fio segura.

Iniciar o Wireless Network Security

O Wireless Network Security é ativado por padrão, mas você pode ativar ou desativar manualmente a proteção sem fio.

Essa proteção defende sua rede sem fio contra invasão e interceptação de dados. Entretanto, se você estiver conectado a uma rede sem fio externa, sua proteção dependerá do nível de segurança dessa rede.

Para ativar manualmente a proteção sem fio:

1 No painel do McAfee Security Center, execute um dos procedimentos a seguir:
   - Clique em **Internet e rede** e, em seguida, em **Configurar**.
   - Clique em **Menu avançado**, depois em **Configurar** no painel **Início** e, em seguida, aponte para **Internet e rede**.
2 No painel **Internet e Configuração de rede**, em **Proteção sem fio**, clique em **Ligado**.

Observação: O Wireless Network Security é ativado automaticamente quando há um adaptador sem fio compatível instalado.

Interromper o Wireless Network Security

O Wireless Network Security é ativado por padrão, mas você pode ativar ou desativar manualmente a proteção sem fio.

Se você desativar a proteção sem fio, sua rede ficará vulnerável a invasão e interceptação de dados.

Para desativar a proteção sem fio:

1 No painel do McAfee Security Center, execute um dos procedimentos a seguir:
   - Clique em **Internet e rede** e, em seguida, em **Configurar**.
   - Clique em **Menu avançado**, depois em **Configurar** no painel **Início** e, em seguida, aponte para **Internet e rede**.

2 No painel **Internet e Configuração de rede**, em **Proteção sem fio**, clique em **Desligado**.

CAPÍTULO 14

Proteção de redes sem fio

O Wireless Network Security protege sua rede implementando criptografia sem fio (seja através de WEP, WPA ou WPA2, dependendo de seu equipamento). Ele programa automaticamente clientes e roteadores em fio com credenciais válidas de chave de criptografia, de modo que o roteador sem fio autorize os computadores a se conectarem. As redes sem fio protegidas com criptografia bloqueiam o acesso de usuários não autorizados à rede e protegem os dados que são enviados por meio de uma rede sem fio. O Wireless Network Security realiza isso da seguinte maneira:

- Criando e distribuindo uma chave de criptografia grande, forte, aleatória e compartilhada
- Alterando a chave de criptografia em períodos programados
- Configurando cada dispositivo sem fio com chaves de criptografia

Neste capítulo

Configurando redes sem fio protegidas

Quando o Wireless Network Security é instalado, ele automaticamente pergunta se você deseja proteger a rede sem fio desprotegida à qual você está conectado ou se deve associar-se a uma rede sem fio previamente protegida.

Se você não estiver conectado a uma rede sem fio, o Wireless Network Security fará uma varredura em busca de uma rede protegida pela McAfee com uma forte intensidade de sinal e solicitará que o usuário se associe a essa rede. Caso não haja redes protegidas, o Wireless Network Security fará a varredura em busca de redes não seguras com sinais fortes e, quando encontrar uma, solicitará que você proteja essa rede.

A menos que uma rede sem fio esteja protegida pelo McAfee Wireless Network Security, o McAfee a considerará “desprotegida” -- mesmo se ela utilizar mecanismos de segurança sem fio, como WEP e WPA.

A menos que uma rede sem fio esteja protegida pelo Wireless Network Security, a McAfee considerará a rede desprotegida, mesmo se ela utilizar um mecanismo de segurança sem fio como WEP e WPA.

Sobre os tipos de acesso

Qualquer computador sem fio com o recurso Wireless Network Security instalado pode criar uma rede sem fio protegida. O primeiro computador a proteger um roteador e a criar uma rede sem fio protegida será automaticamente atribuído ao acesso administrativo dessa rede. Um usuário com acesso administrativo pode atribuir acesso administrativo, total ou de convidado aos computadores que entram posteriormente.

Computadores com tipos de acesso administrativo ou total podem executar as seguintes tarefas:

- Proteger ou remover um roteador ou ponto de acesso
- Fazer a rotação de chaves de segurança
- Alterar as configurações de segurança da rede
- Reparar redes
- Conceder aos computadores o acesso à rede
- Revogar o acesso à rede sem fio protegida
- Alterar o nível de administração de um computador

Computadores com tipos de acesso convidado podem executar as seguintes tarefas na rede:

- Conectar-se a uma rede
- Associar-se a uma rede
- Modificar as configurações específicas no computador convidado

Observação: Os computadores podem ter acesso administrativo em uma rede sem fio, mas podem ter acesso de convidado ou total em outra. Um computador com acesso de convidado ou total em uma rede pode criar uma nova rede.

Tópicos relacionados

- Associar-se a uma rede sem fio protegida (página 82)
- Conceder acesso administrativo a computadores (página 86)
- Revogar acesso à rede (página 103)

Criar redes sem fio protegidas

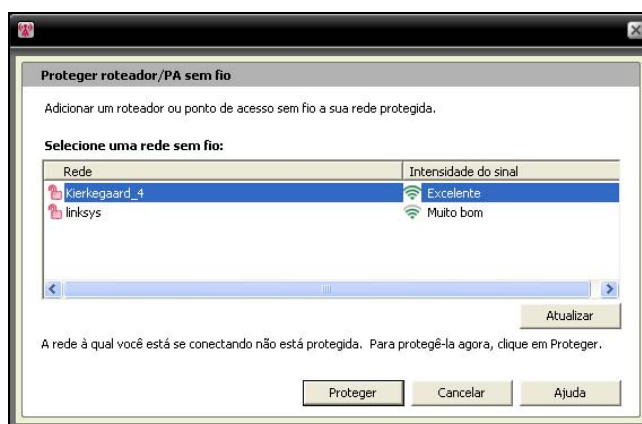
Para criar uma rede sem fio protegida, é necessário primeiro adicionar o roteador ou ponto de acesso sem fio da rede.

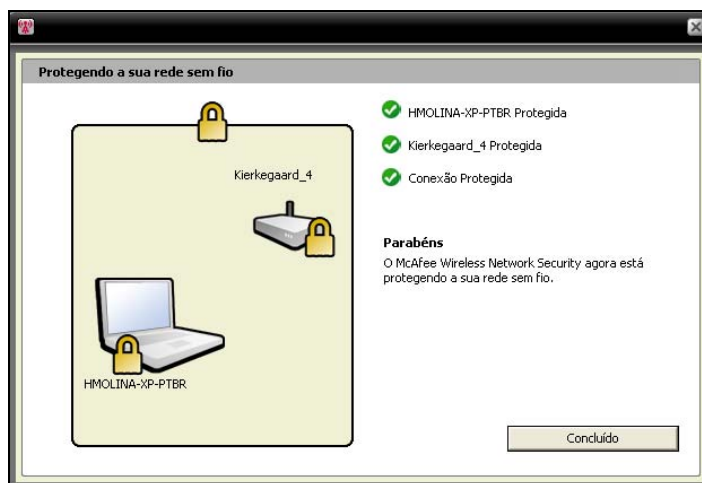
Para adicionar um roteador ou ponto de acesso sem fio:

1 Clique com o botão direito do mouse no ícone do Wireless Network Security, na área de notificação do Windows.

2 Selecione **Exibir ferramentas**.

3 No painel de Ferramentas de proteção, em **Proteger roteador/PA sem fio**, clique em **Proteger**.

4 No painel Proteger roteador/PA sem fio, selecione um rede sem fio a ser protegida e, então, clique em **Proteger**.

O painel Protegendo a sua rede sem fio aparece quando o Wireless Network Security tenta proteger seu computador, roteador ou conexão da rede.

A proteção bem-sucedida de todos esses componentes resulta em uma proteção total de sua rede sem fio.

5 Clique em **Concluído**.

Observação: Depois que você proteger uma rede, a caixa de diálogo Suas próximas etapas lembrará a você que o Wireless Network Security deve ser instalado em cada um dos computadores sem fio para permitir que eles se associem à rede.

Se antes você configurou manualmente uma chave pré-compartilhada de seu roteador ou ponto de acesso e não estava conectado quando tentou proteger o roteador ou ponto de acesso, será necessário também digitar a chave na caixa Chave de WEP e, então, clicar em Conectar. Se você alterou previamente o nome de usuário administrativo ou a senha de seu roteador sem fio, será solicitado que digite essa informação antes de proteger um roteador ou ponto de acesso.

Tópicos relacionados

- Proteger outros dispositivos sem fio (página 87)
- Adicionar computadores à rede sem fio protegida (página 89)

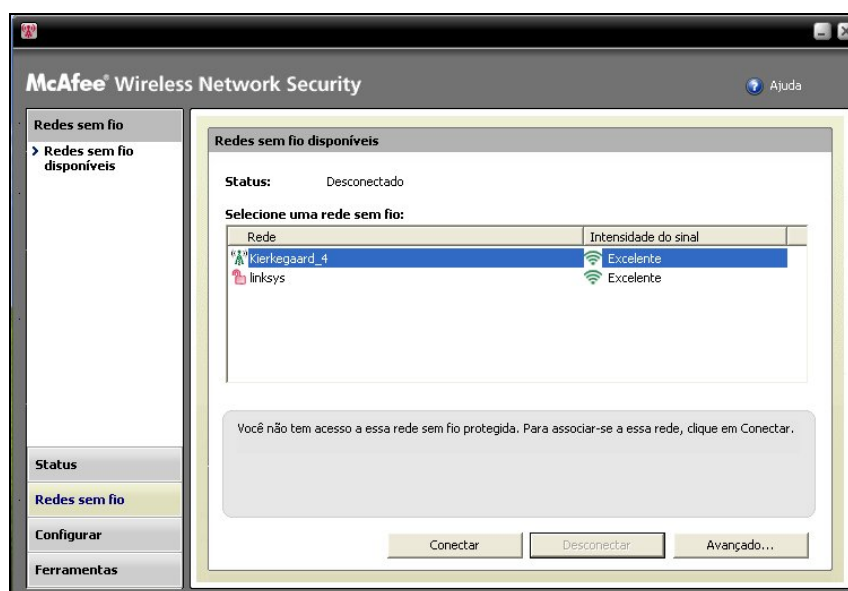
Associar-se a redes sem fio protegidas

Uma rede protegida impede que hackers interceptem dados transmitidos e que se conectem a ela. Para que um computador autorizado possa acessar uma rede sem fio protegida, primeiro ele precisa ser associado a ela.

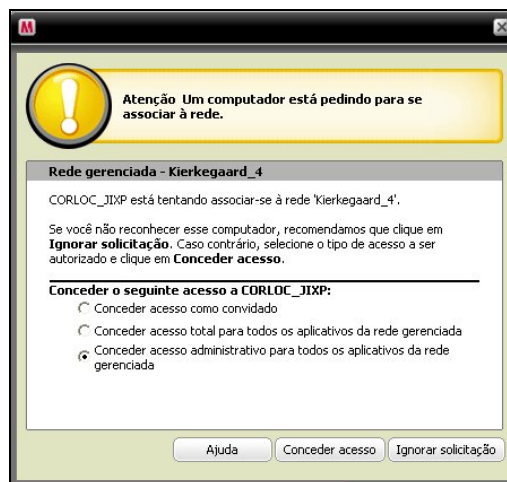
Quando um computador solicita associar-se à rede gerenciada, uma mensagem é enviada aos outros computadores da rede que têm acesso administrativo. Como administrador, você é responsável por decidir que tipo de acesso deve ser concedido ao computador: convidado, total ou administrativo.

Antes de ser associado a uma rede protegida, você deve instalar o Wireless Network Security e, então, conectar-se à rede sem fio protegida. Um usuário já existente com acesso administrativo na rede sem fio protegida deve permitir que você se associe. Após associar-se à rede, não é necessário mais associar-se a ela novamente quando se reconectar. Tanto o concessor quanto o associado devem ter uma conexão sem fio ativa. O concessor deve ter um computador administrativo conectado à rede.

Para associar-se a uma rede sem fio protegida:

1. No computador desprotegido, clique com o botão direito do mouse no ícone do Wireless Network Security, na área de notificação do Windows.
2. Selecione **Exibir redes sem fio**.
3. No painel Redes sem fio disponíveis, selecione uma rede e clique em **Conectar**.

4 Na caixa de diálogo Associar-se à rede sem fio protegida, clique em **Sim** para associar-se à rede.

Enquanto o Wireless Network Security tenta obter permissão para associar-se à rede, o painel Associando-se a uma rede sem fio protegida aparece no computador que está tentanto associar-se à rede.

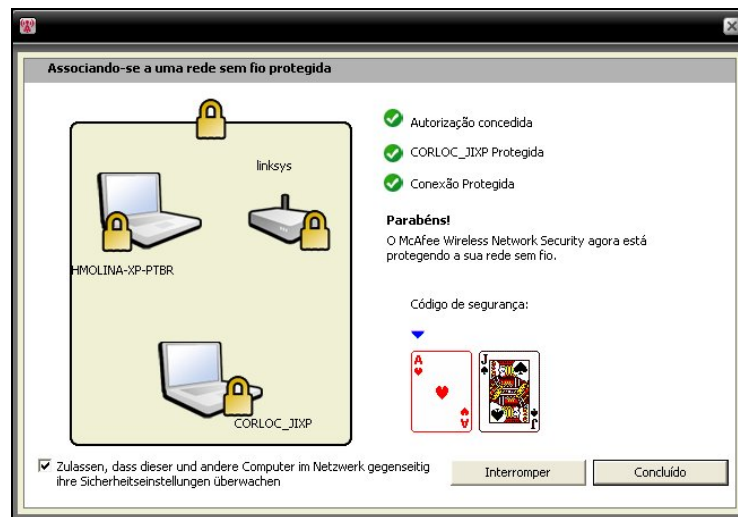
5 O painel Associar-se à rede aparece no computador administrativo a partir do qual pode ser atribuído acesso de convidado, total ou administrativo.

Na caixa de diálogo Associar-se à rede, selecione uma das seguintes opções:

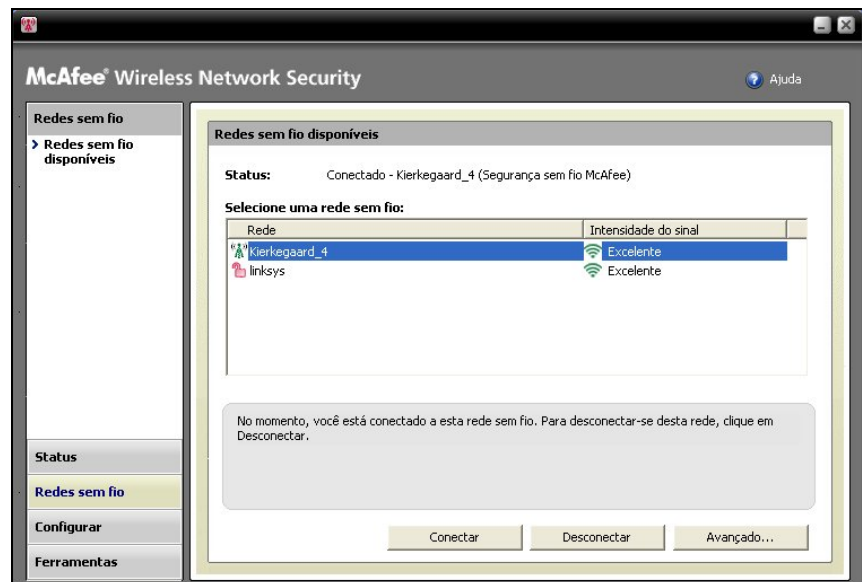
Conceder acesso como convidado	Permite que o computador envie arquivos a outros computadores na rede sem fio, mas não permite compartilhar arquivos com o McAfee EasyNetwork.
Conceder acesso total para todos os aplicativos da rede gerenciada	Permite que o computador envie e compartilhe arquivos com o McAfee EasyNetwork.
Conceder acesso administrativo para todos os aplicativos da rede gerenciada	Permite que o computador envie e compartilhe arquivos com o McAfee EasyNetwork, conceda acesso a outros computadores e ajuste os níveis de acesso de outros computadores na rede sem fio.

6 Clique em **Conceder acesso**.

7 Confirme se as cartas exibidas no painel Concedendo acesso de rede correspondem àquelas exibidas no computador que está tentando associar-se à rede sem fio. Se as cartas corresponderem, clique em **Conceder acesso**.

Se os computadores não exibirem cartas idênticas, terá ocorrido uma potencial violação de segurança. A concessão de acesso desse computador à rede pode colocá-lo em risco. Para proibir que o computador acesse a rede sem fio, clique em **Rejeitar acesso**.

8 O painel Concedendo acesso de rede confirma se o novo computador está protegido pelo Wireless Network Security. Para monitorar as configurações de segurança de outros computadores, e para ser monitorado por eles, selecione **Permitir que este computador e outros computadores da rede monitorem as configurações de segurança uns dos outros**.

9 Clique em **Concluído**.

10 O painel Redes sem fio disponíveis mostra que você está conectado à rede sem fio protegida.

Tópicos relacionados

- Adicionar computadores à rede sem fio protegida (página 89)

Conectar-se a redes sem fio protegidas

Se você já se associou a uma rede sem fio protegida, mas depois se desconectou e seu acesso não foi revogado, você poderá se reconectar a qualquer momento sem precisar de nova associação.

Para se conectar a uma rede sem fio protegida:

1 Clique com o botão direito do mouse no ícone do Wireless Network Security, na área de notificação do Windows.

2 Selecione **Exibir redes sem fio**.

3 No painel Redes sem fio disponíveis, selecione uma rede e clique em **Conectar**.

Conceder acesso administrativo a computadores

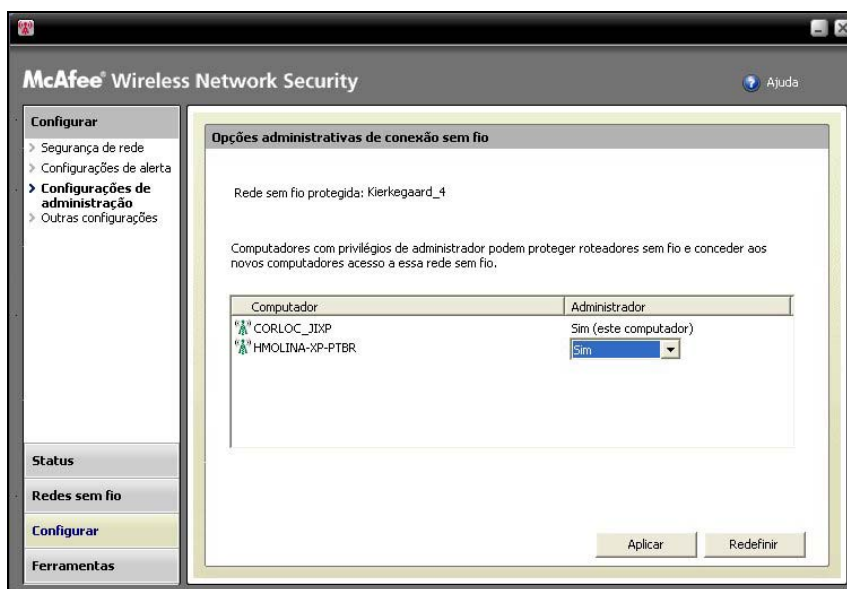
Computadores com privilégios administratiivos podem proteger roteadores sem fio, alterar modos de segurança e conceder aos novos computadores acesso a essa rede sem fio protegida.

Para configurar acesso administrativo:

1 Clique com o botão direito do mouse no ícone do Wireless Network Security, na área de notificação do Windows.

2 Selecione **Exibir configuração**.

3 No painel Configurar, selecione **Configurações administrativas**.

4 No painel Opções de administração sem fio, selecione **Sim** ou **Não** para permitir ou não o acesso administrativo.

5 Clique em **Aplicar**.

Tópicos relacionados

- Sobre os tipos de acesso (página 79)
- Revogar acesso à rede (página 103)

Proteger outros dispositivos sem fio

O Wireless Network Security permite que você adicione uma ou mais impressoras, servidores de impressão ou consoles de jogos sem fio à rede.

Para adicionar uma impressora sem fio, um servidor de impressão ou um console de jogos:

1. Clique com o botão direito do mouse no ícone do Wireless Network Security, na área de notificação do Windows.
2. Selecione **Exibir ferramentas**.
3. No painel Ferramentas de proteção, em **Proteger dispositivos sem PA**, clique em **Proteger**.
4. No painel Proteger um dispositivo sem fio, selecione um dispositivo sem fio e clique em **Proteger**.
5. O alerta Dispositivo sem PA protegido confirma que o dispositivo foi adicionado à rede.

Conectar a redes com Difusão de SSID desativada

Você pode conectar a redes sem fio em que a Difusão de SSID está desativada. Quando os roteadores desativam a Difusão de SSID, não aparecem no painel de Redes sem fio disponíveis.

A McAfee recomenda que você não proteja com o Wireless Network Security os roteadores sem fio em que a Difusão de SSID esteja desativada.

Para conectar-se a uma rede sem fio com Difusão de SSID desativada:

1. Clique com o botão direito do mouse no ícone do Wireless Network Security, na área de notificação do Windows.
2. Selecione **Exibir redes sem fio**.
3. No painel Redes sem fio disponíveis, clique em **Avançado**.
4. No painel Redes sem fio, clique em **Adicionar**.
5. No painel Adicionar rede sem fio, especifique as seguintes configurações e clique em **OK**:

Configuração	Descrição
Rede	O nome de sua rede. Se estiver modificando uma rede, você não pode mudar o nome.
Configurações de segurança	A segurança para sua rede desprotegida. Observe que, se o adaptador sem fio não suportar o modo selecionado, não será possível fazer a conexão. Os modos de segurança são: Desativado, WEP aberta, WEP compartilhada, WEP automática, WPA-PSK, WPA2-PSK.
Modo de criptografia	A criptografia associada ao modo de segurança selecionado. Os modos de criptografia são: WEP, TKIP, AES, e TKIP+AES.

Observação: A McAfee recomenda que você não proteja com o Wireless Network Security os roteadores sem fio em que a Difusão de SSID esteja desativada. Se precisar utilizar esse recurso, somente o faça quando a difusão de SSID estiver desativada.

Adicionar computadores à rede sem fio protegida

Você pode adicionar computadores à rede sem fio protegida usando um dispositivo removível, como uma unidade flash USB, CD gravável ou tecnologia Windows Connect Now.

Adicionar computadores usando um dispositivo removível

O Wireless Network Security permite incluir computadores adicionais à rede sem fio protegida que não executam o Wireless Network Security, usando uma unidade flash USB ou um CD gravável.

Para adicionar um computador:

1. Clique com o botão direito do mouse no ícone do Wireless Network Security, na área de notificação do Windows.
2. Selecione **Exibir ferramentas**.
3. No painel Ferramentas de proteção, em **Proteger um computador**, clique em **Proteger**.
4. No painel Proteger um outro computador, selecione **Copie o Wireless Network Security em um dispositivo removível, como uma chave USB**.

5 Selecione um local da Unidade de CD ou unidade flash USB para copiar o Wireless Network Security.

6 Clique em **Copiar**.

7 Após copiar todos os arquivos para o CD ou a unidade flash USB, insira o dispositivo removível no computador que deseja proteger. Se o programa não iniciar automaticamente, vá para o conteúdo da mídia removível no Windows Explorer e clique em **Install.exe**.

8 Siga as instruções da tela.

Observação: Você também pode adicionar um computador à rede sem fio protegida usando a tecnologia Windows Connect Now.

Tópicos relacionados

- Adicionar computadores usando a tecnologia Windows Connect Now (página 91)

Adicionar computadores usando a tecnologia Windows Connect Now.

O Wireless Network Security permite incluir em sua rede computadores adicionais que não estejam executando o Wireless Network Security, por meio da tecnologia Windows Connect Now.

Para adicionar um computador usando a tecnologia Windows Connect Now:

1. Clique com o botão direito do mouse no ícone do Wireless Network Security, na área de notificação do Windows.
2. Selecione **Exibir ferramentas**.
3. No painel Ferramentas de proteção, em **Proteger um computador**, clique em **Proteger**.
4. No painel Proteger um outro computador, selecione **Criar um disco Windows Connect Now**.
5. Selecione um local para copiar as informações do Windows Connect Now.
6. Clique em **Copiar**.
7. Insira o disco Windows Connect Now no computador que deseja proteger.
8. Se o disco não iniciar automaticamente, execute um dos procedimentos a seguir:
   - Instale a tecnologia sem fio Connect Now: Clique em **Iniciar** na barra de tarefas do Windows e, em seguida, clique em Painel de Controle. Se estiver usando a exibição de Categoria do Painel de Controle, clique em **Conexões de rede e Internet** e, em seguida, clique em **Assistente de configuração de rede sem fio**. Se estiver usando a exibição Clássica do Painel de Controle, clique em **Assistente de configuração de rede**. Siga as instruções da tela.
   - Abra `setupSNK.exe` no disco de Conexão do Windows e copie e cole a chave para seu cliente de seleção de rede sem fio.

Observação: Suspenda a rotação de chaves se você usa a tecnologia Windows Connect para conectar a rede sem fio, caso contrário sua conexão de rede falhará. Ocorre falha na conexão porque a rotação de chaves cria uma nova chave que difere da chave utilizada pela tecnologia Windows Connect Now.

Você pode adicionar computadores à rede sem fio protegida usando um dispositivo removível, como um CD gravável ou uma unidade flash USB.

Tópicos relacionados

- Adicionar computadores usando um dispositivo removível (página 89)

CAPÍTULO 15

Administrando redes sem fio

O Wireless Network Security fornece um conjunto completo de ferramentas de administração para ajudar você a gerenciar e manter sua rede sem fio.

Neste capítulo

Gerenciamento de redes sem fio

Quando você está conectado a uma rede sem fio protegida, as informações enviadas e recebidas são criptografadas. Hackers não podem descriptografar os dados transmitidos através da rede protegida e não podem se conectar à sua rede. O Wireless Network Security fornece várias ferramentas para ajudar você a gerenciar sua rede e evitar intrusões.

Sobre os ícones do Wireless Network Security

O Wireless Network Security exibe ícones para representar vários tipos de conexão de rede e várias intensidades de sinal.

Ícones de conexão de rede

A tabela a seguir descreve os ícones geralmente utilizados pelo Wireless Network Security nos painéis Status da rede sem fio e nos painéis Ferramentas de proteção e Redes sem fio disponíveis. Os ícones representam vários estados da conexão de rede e da segurança.

Ícone	Painéis de status	Painéis de proteção
	Seu computador está conectado à rede sem fio protegida selecionada.	O dispositivo é protegido pelo Wireless Network Security.
	Seu computador pode acessar a rede sem fio protegida, mas não está conectado no momento.	O dispositivo utiliza a segurança WEP ou WPA.
	Seu computador é antigo membro da rede sem fio protegida, mas o acesso foi revogado quando o computador estava desconectado da rede.	O Wireless Network Security está desativado no dispositivo.

Ícones de intensidade do sinal

A tabela a seguir descreve os ícones geralmente utilizados pelo Wireless Network Security para representar várias intensidades de sinal da rede.

Ícone	Descrição
	Intensidade de sinal excelente
	Intensidade de sinal muito boa
	Intensidade de sinal boa
	Intensidade de sinal baixa

Tópicos relacionados

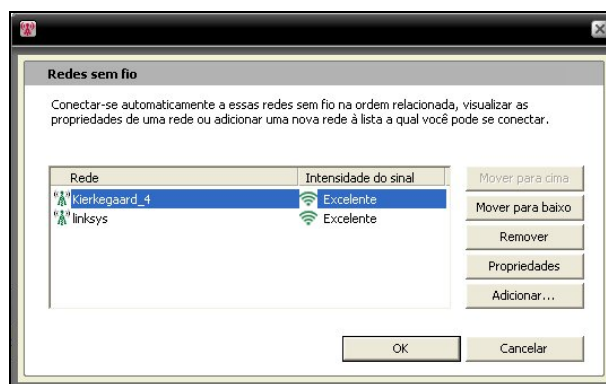
- Exibir a intensidade do sinal da rede (página 125)
- Exibir computadores protegidos no momento (página 131)
- Exibir o modo de segurança da rede (página 124)

Listar redes preferidas

O Wireless Network Security permite que você especifique redes sem fio preferidas. Isso permite que você especifique a ordem das redes às quais seu computador é conectado automaticamente. O Wireless Network Security tenta conectar a primeira rede que aparece na lista.

Esse recurso é útil quando, por exemplo, você deseja conectar-se automaticamente à rede sem fio de seu amigo quando está na área dele. Você pode colocar outra rede no topo da lista.

Para relacionar redes preferidas:

1. Clique com o botão direito do mouse no ícone do Wireless Network Security, na área de notificação do Windows.
2. Selecione **Exibir redes sem fio**.
3. No painel Redes sem fio disponíveis, clique em **Avançado**.
4. Selecione a rede na ordem em que você deseja ajustar e clique em **Mover para cima** ou **Mover para baixo**.

5. Clique em **OK**.

Tópicos relacionados

- Remover redes sem fio preferidas (página 97)

Remover redes sem fio preferidas

Você pode utilizar o Wireless Network Security para remover redes preferidas.

Isso é útil quando, por exemplo, você deseja remover uma rede obsoleta da lista.

Para remover redes preferidas:

1 Clique com o botão direito do mouse no ícone do Wireless Network Security, na área de notificação do Windows.

2 Selecione **Exibir redes sem fio**.

3 No painel Redes sem fio disponíveis, clique em **Avançado**.

4 No painel Redes sem fio, selecione uma rede e clique em **Remover**.

5 Clique em **OK**.

Tópicos relacionados

- Listar redes preferidas (página 96)

Renomear redes sem fio protegidas

Você pode utilizar o Wireless Network Security para renomear sua rede sem fio protegida já existente.

Renomear a rede poderá ser útil caso seu nome seja semelhante ou idêntico ao de uma rede utilizada por seu vizinho ou se você deseja criar um nome exclusivo para ficar mais fácil sua distinção.

Talvez seja necessário reconectar os computadores conectados à rede sem fio protegida manualmente. Eles são notificados quando o nome é alterado.

Depois de renomear a rede, o novo nome aparece no painel Roteador/PA sem fio protegido.

Para modificar o nome de sua rede sem fio protegida:

1 Clique com o botão direito do mouse no ícone do Wireless Network Security, na área de notificação do Windows.

2 Selecione **Exibir configuração**.

3 No painel Segurança da rede, digite o novo nome na caixa **Nome da rede sem fio protegida**.

4 Clique em **Aplicar**.

   A caixa de diálogo Atualizando configurações de segurança da rede é exibida quando o Wireless Network Security altera o nome da rede sem fio protegida. Dependendo das configurações de seu computador e da intensidade do sinal, o nome da rede será alterado em menos de um minuto.

Observação: Como medida de segurança, a McAfee recomenda renomear o SSID padrão do roteador ou do ponto de acesso. Embora o Wireless Network Security suporte SSIDs padrões como "linksys," ou "belkin54g" ou "NETGEAR", a renomeação de SSIDs protege você contra ameaças de pontos de acesso não confiáveis.

Definir configurações de alerta

O Wireless Network Security permite que você defina as configurações de alerta para exibir alertas quando ocorrem certos eventos, como quando um novo computador é conectado à sua rede.

Para definir o comportamento dos alertas:

1 Clique com o botão direito do mouse no ícone do Wireless Network Security, na área de notificação do Windows.

2 Selecione **Exibir configuração**.

3 Clique em **Configurações de alerta**.

4 Selecione ou desmarque um dos seguintes eventos e clique em **Aplicar**:

Configuração de alerta	Descrição
Rotação da chave de segurança para a sua rede sem fio protegida	Exibe o alerta de Chave de segurança trocada após a rotação manual ou automática da chave de segurança. A rotação da chave protege sua rede contra tentativas de hackers de interceptar seus dados ou conectar à sua rede.
Um outro computador protegido é conectado ou desconectado da rede	Exibe o alerta de Computador conectado ou Computador desconectado depois que um computador é conectado ou desconectado da rede sem fio protegida. Os dados nos computadores conectados estão agora protegidos contra intrusões e interceptações.
É concedido acesso a um outro computador à sua rede sem fio protegida	Exibe o alerta de Acesso de rede concedido ao computador depois que um computador administrador permite que outro computador entre na rede sem fio protegida. Conceder acesso do computador à rede protegida protege o computador contra tentativas de hackers de interceptar seus dados.
A rotação de chaves para a sua rede sem fio protegida é suspensa ou retomada	Exibe o alerta de Rotação de chaves suspensa ou Rotação de chaves retomada após suspender ou retomar manualmente a rotação de chaves. A rotação da chave protege sua rede contra tentativas de hackers de interceptar seus dados ou conectar-se à sua rede.
O acesso é revogado em todos os computadores desconectados	Exibe o alerta de Acesso revogado depois que o acesso de computadores não conectados à rede é revogado. Computadores desconectados devem ser associados novamente à rede.
Um roteador é adicionado ou removido da sua rede sem fio protegida	Exibe o alerta de Roteador/PA adicionado à rede ou de Roteador/PA desprotegido após o roteador ou o ponto de acesso sem fio ser adicionado ou removido da rede sem fio protegida.
As informações de logon de um roteador sem fio protegido são alteradas	Exibe o alerta de Logon do roteador/PA alterado depois que o administrador do Wireless Network Security altera o nome do usuário ou a senha de um roteador ou ponto de acesso.

A configuração de segurança ou nome da sua rede sem fio protegida são alterados	Exibe o alerta de Configurações da rede alteradas ou Rede renomeada depois que você renomeia a rede sem fio protegida ou ajusta suas configurações de segurança.
As configurações da sua rede sem fio protegida são reparadas	Exibe o alerta de Rede reparada quando as configurações de segurança nos roteadores ou pontos de acesso sem fio de sua rede são corrigidas.

Observação: Para escolher ou desmarcar todas as configurações de alerta, clique em **Selecionar tudo** ou **Limpar tudo**. Para redefinir as configurações de alerta do Wireless Network Security, clique em **Restaurar padrões**.

Tópicos relacionados

- Rotação automática das chaves (página 112)
- Associar-se a uma rede sem fio protegida (página 82)
- Conectar-se a redes sem fio protegidas (página 86)
- Desconectar de redes sem fio protegidas (página 102)
- Suspender a rotação de chaves automática (página 115)
- Revogar acesso à rede (página 103)
- Remover roteadores ou pontos de acesso sem fio (página 101)
- Alterar as credenciais para dispositivos sem fio (página 109)
- Renomear redes sem fio protegidas (página 97)
- Reparar configurações de segurança da rede (página 110)

Exibir notificações de conexão

Você pode configurar o Wireless Network Security para notificar quando seu computador se conectar a uma rede sem fio.

Para exibir notificação ao se conectar a uma rede sem fio:

1. Clique com o botão direito do mouse no ícone do Wireless Network Security, na área de notificação do Windows.
2. Selecione **Exibir configuração**.
3. Clique em **Outras configurações**.
4. Selecione **Exibir mensagem de notificação quando conectado a uma rede sem fio**.
5. Clique em **Aplicar**.

Tópicos relacionados

- Conectar-se a redes sem fio protegidas (página 86)

Remover roteadores ou pontos de acesso sem fio

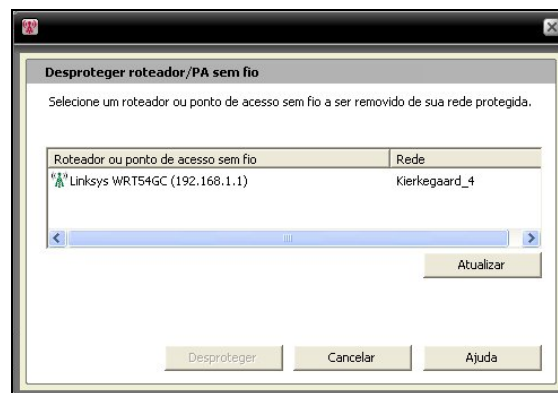
O Wireless Network Security permite remover um ou mais roteadores ou pontos de acesso de sua rede protegida.

Para remover um roteador ou ponto de acesso sem fio:

1 Clique com o botão direito do mouse no ícone do Wireless Network Security, na área de notificação do Windows.

2 Selecione **Exibir ferramentas**.

3 No painel Ferramentas de proteção, em **Desproteger um dispositivo**, clique em **Desproteger**.

4 No painel Desproteger roteador/PA sem fio, selecione um roteador ou ponto de acesso sem fio para remover da rede protegida e clique em **Desproteger**.

5 Clique em **OK** na caxia de diálogo Roteador/PA sem fio desprotegido para confirmar que o roteador ou ponto de acesso sem fio foi removido da rede.

Tópicos relacionados

- Criar redes sem fio protegidas (página 80)

Desconectar de redes sem fio protegidas

O Wireless Network Security permite desconectar seu computador da rede.

Essa tarefa é útil quando, por exemplo, seu computador tiver se conectado a uma rede usando um nome idêntico ao seu nome de rede. Você pode desconectar da rede e, em seguida, reconectar-se.

Esse recurso é útil, também, quando você se conecta acidentalmente a uma rede errada, ou porque a intensidade do outro ponto de acesso é forte ou como resultado de interferência de rádio.

Para se desconectar a uma rede sem fio protegida:

1 Clique com o botão direito do mouse no ícone do Wireless Network Security, na área de notificação do Windows.

2 Selecione **Exibir redes sem fio**.

3 No painel Redes sem fio disponíveis, selecione a rede e clique em **Desconectar**.

Tópicos relacionados

- Revogar acesso à rede (página 103)
- Sair de redes sem fio protegidas (página 104)

Revogar acesso à rede

O Wireless Network Security permite revogar o acesso de computadores que não estão conectados à rede. Uma nova programação de rotação de chave de segurança é estabelecida: computadores não conectados perderão o acesso à rede sem fio protegida, mas poderão recuperá-lo quando se associarem novamente na rede. O acesso dos computadores conectados é mantido.

Por exemplo, você pode revogar o acesso do computador de um visitante com o Wireless Network Security depois que ele se desconectar. Além disso, um adulto pode revogar o acesso de um computador utilizado por uma criança como forma de controle de restrição para menores ao acesso à Internet. O acesso de um computador que foi concedido acidentalmente também pode ser revogado.

Para revogar o acesso de todos os computadores desconectados da rede protegida:

1 Clique com o botão direito do mouse no ícone do Wireless Network Security, na área de notificação do Windows.

2 Selecione **Exibir ferramentas**.

3 No painel Ferramentas, clique em Ferramentas de manutenção.

4 No painel Ferramentas de manutenção, em **Revogar acesso**, clique em **Revogar**.

5 No painel Revogar acesso, clique em **Revogar**.

6 Clique em **OK** na caixa de diálogo Wireless Network Security.

Tópicos relacionados

- Desconectar de redes sem fio protegidas (página 102)
- Sair de redes sem fio protegidas (página 104)

Sair de redes sem fio protegidas

Você pode usar o Wireless Network Security para cancelar seus direitos de acesso a uma rede protegida.

Para sair de uma rede:

1. Clique com o botão direito do mouse no ícone do Wireless Network Security, na área de notificação do Windows.
2. Selecione **Exibir configuração**.
3. No painel de Configurar, selecione **Outras configurações**.
4. No painel Outras configurações, em Acesso à rede protegida, selecione a rede que deseja deixar e clique em **Sair da rede**.
5. No painel Desconectar da rede, clique em **Sim** para sair da rede.

Observação: Para que você se associe novamente a uma rede depois de sair dela, é necessário que outro usuário conceda a você o acesso à rede protegida.

Tópicos relacionados

- Desconectar de redes sem fio protegidas (página 102)
- Revogar acesso à rede (página 103)

CAPÍTULO 16

Gerenciando a segurança da rede sem fio

O Wireless Network Security fornece um conjunto completo de ferramentas para ajudar você a gerenciar os recursos de segurança de sua rede sem fio.

Neste capítulo

Definição de configurações de segurança

Após conectar-se a uma rede sem fio protegida, o Wireless Network Security automaticamente protege sua rede, entretanto, você pode definir configurações adicionais de segurança a qualquer momento.

Configurar modos de segurança

Você pode especificar o modo de segurança de sua rede sem fio protegida. Os modos de segurança definem a criptografia entre seu computador e o roteador ou ponto de acesso.

Quando você protege sua rede, o WEP é configurado automaticamente. Entretanto, a McAfee recomenda que você mude o modo de segurança para WPA2 ou WPA-PSK AES. O Wireless Network Security utiliza WEP inicialmente porque esse modo é suportado por todos os roteadores e adaptadores de rede sem fio. Muitos novos roteadores e adaptadores de rede sem fio, contudo, trabalham no modo WPA, que é mais seguro.

Para alterar o modo de segurança de uma rede sem fio protegida:

1. Clique com o botão direito do mouse no ícone do Wireless Network Security, na área de notificação do Windows.
2. Selecione **Exibir configuração**.
3. No painel Segurança da rede, selecione o tipo de segurança que deseja implementar na caixa **Modo de segurança** e clique em **Aplicar**.

A tabela a seguir descreve os modos de segurança disponíveis:

Intensidade	Modo	Descrição
Mais fraca	WEP	WEP (Wired Equivalent Privacy) é parte do padrão de rede sem fio IEEE 802.11 para proteger redes sem fio IEEE 802.11. A WEP fornece um nível de segurança que pode evitar espionagens não sofisticadas, mas geralmente não é tão seguro quanto a criptografia WPA-PSK. Embora o Wireless Network Security ofereça uma chave forte (difícil de adivinhar e grande), a McAfee recomenda utilizar um modo de segurança WPA.
Média	WPA-PSK TKIP	WPA (Wi-Fi Protected Access) é uma versão anterior do padrão de segurança 802.11i. TKIP é projetado para WPA para aprimorar a WEP. TKIP fornece integridade de mensagem, mecanismo de recriação de chaves e mistura de chaves por pacote
Forte	WPA-PSK AES	Esse modo de segurança combina os modos WPA e AES. O AES (Advanced Encryption Standard) é um código de bloqueio adotado como um padrão de criptografia pelo governo dos Estados Unidos.
Mais forte	WPA2-PSK AES	Esse modo de segurança combina os modos WPA2 e AES. O modo WPA2 é o próximo avanço da ratificação do padrão de segurança 802.11i. O WPA2 emprega o CCMP (Counter Mode CBC MAC Protocol), que é uma solução mais segura e escalável quando comparada ao TKIP. Esse é o modo de segurança mais forte disponível aos consumidores.
A mais forte de todas	WPA2-PSK TKIP+AES	Esse modo de segurança combina os modos WPA2 e AES, bem como WPA-PSK TKIP. Permite uma maior flexibilidade, por isso tanto os adaptadores sem fio antigos quanto os novos podem ser conectados.

Observação: Após alterar o modo de segurança, pode ser necessário reconectar-se manualmente.

Tópicos relacionados

- Reparar configurações de segurança da rede (página 110)
- Exibir o modo de segurança da rede (página 124)

Definir configurações de segurança da rede

Você pode modificar as propriedades de redes protegidas pelo Wireless Network Security. Isso é útil quando, por exemplo, você deseja fazer o upgrade da segurança de WEP para WPA.

A McAfee recomenda modificar as configurações de segurança da rede se um alerta sugerir que você o faça.

Para configurar as propriedades da rede desprotegida:

1. Clique com o botão direito do mouse no ícone do Wireless Network Security, na área de notificação do Windows.
2. Selecione **Exibir redes sem fio**.
3. No painel Redes sem fio disponíveis, clique em **Avançado**.
4. No painel Redes sem fio, clique em **Propriedades**.
5. No painel Propriedades da rede sem fio, modifique as seguintes configurações e então clique em **OK**:

Configuração	Descrição
Rede	O nome de sua rede. Se estiver modificando uma rede, você não poderá mudar o nome.
Configurações de segurança	A segurança para sua rede desprotegida. Observe que, se o adaptador sem fio não suportar o modo selecionado, não será possível fazer a conexão. Os modos de segurança são: Desativado, WEP aberta, WEP compartilhada, WEP automática, WPA-PSK, WPA2-PSK.
Modo de criptografia	A criptografia associada ao modo de segurança selecionado. Os modos de criptografia são: WEP, TKIP, AES e TKIP+AES.

Alterar as credenciais para dispositivos sem fio

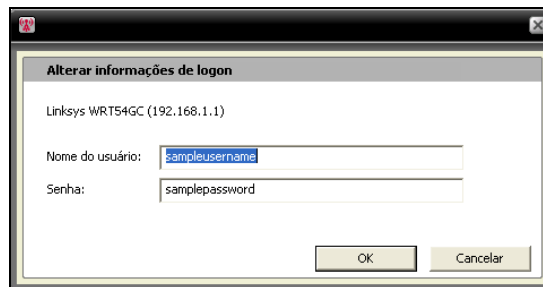
Você pode alterar o nome do usuário ou a senha de um dispositivo em seu roteador ou ponto de acesso sem fio protegido. A lista de dispositivos aparece sob **Dispositivos na rede sem fio protegida**.

A McAfee recomenda alterar suas credenciais porque a maior parte dos dispositivos sem fio de um único fabricante possui as mesmas credenciais de logon. A mudança das credenciais de logon ajuda a impedir o acesso de seu roteador ou ponto de acesso sem fio e a alteração de suas configurações.

Para alterar o nome do usuário ou a senha de um dispositivo de rede sem fio protegida:

1 Clique com o botão direito do mouse no ícone do Wireless Network Security, na área de notificação do Windows.

2 Selecione **Exibir configuração**.

3 No painel de Segurança da rede, sob **Dispositivos na rede sem fio protegida**, selecione um roteador ou ponto de acesso sem fio e clique em **Alterar nome do usuário ou senha**.

4 Clique em **OK** na caixa de diálogo Wireless Network Security após digitar suas informações de logon.

O novo nome do usuário e senha aparecem em **Dispositivos na rede sem fio protegida**.

Observação: Alguns roteadores não suportam nomes de usuários e, portanto, um nome do usuário não aparecerá em **Dispositivos na rede sem fio protegida**.

Reparar configurações de segurança da rede

Se estiver com problemas nas suas definições ou configurações de segurança, você poderá utilizar o Wireless Network Security para reparar as configurações de seu roteador ou ponto de acesso.

Para reparar suas configurações de segurança:

1. Clique com o botão direito do mouse no ícone do Wireless Network Security, na área de notificação do Windows.
2. Selecione **Exibir ferramentas**.
3. No painel Ferramentas, clique em **Ferramentas de manutenção**.
4. Em **Reparar configurações de segurança da rede**, clique em **Reparar**.
5. No painel Reparar configurações de segurança da rede, clique em **Reparar**.

   Um alerta do Wireless Network Security indica se a rede foi ou não reparada.

Observação: Se a tentativa de reparar sua rede não for bem-sucedida, conecte-se à rede utilizando um cabo e tente novamente. Se a senha do roteador ou do ponto de acesso tiver sido alterada, você deverá digitá-la novamente para conectar-se.

Administrando chaves de rede

O Wireless Network Security gera chaves de criptografia grandes, fortes e aleatórias com um gerador de chaves aleatórias. Com WEP, a chave é convertida em um valor hexadecimal de 26 dígitos (para 104 bits de entropia, ou força, a força máxima suportada por WEP de 128 bits), ao passo que, com WPA, a chave é uma cadeia ASCII de 63 caracteres. Cada caractere possui 64 valores possíveis (6 bits), fornecendo 384 bits de entropia, o que excede a intensidade de chave WAP de 256 bits.

Ao gerenciar chaves de rede, você poderá exibir as chaves em texto simples ou com asteriscos para pontos de acesso não protegidos, descartar chaves salvas para pontos de acesso não protegidos, ativar ou desativar a rotação de chaves, alterar a freqüência da rotação de chaves, fazer a rotação de chaves manualmente e suspender a rotação de chaves.

Quando a rotação de chaves é feita automaticamente, as ferramentas do hacker não podem capturar as informações porque a chave está sempre sendo alterada.

Entretanto, se você estiver conectando dispositivos sem fio não suportados pelo Wireless Network Security (por exemplo, conectando um computador handheld sem fio à sua rede), será necessário anotar a chave, interromper a rotação de chaves e, então, inseri-la no dispositivo.

Exibir chaves atuais

O Wireless Network Security fornece acesso rápido às informações de segurança sem fio, incluindo a chave atual de uma rede sem fio protegida.

Para exibir a chave atual:

1. Clique com o botão direito do mouse no ícone do Wireless Network Security na área de notificação do Windows.
2. Selecione **Exibir status**.
3. No painel Status da rede sem fio, sob o painel Rede sem fio protegida, clique em **Chave atual**.

   A chave configurada para sua rede aparece na caixa de diálogo Configuração da chave.

Tópicos relacionados

- Exibir o número de rotações de chave (página 128)

Rotação automática das chaves

A rotação de chaves automática é ativada por padrão; entretanto, se você suspender a rotação de chaves, um computador com acesso administrativo poderá reativá-la porteriormente.

Você pode configurar o Wireless Network Security para fazer a rotação de chaves de segurança automaticamente na rede sem fio protegida.

O Wireless Network Security gera automaticamente uma série infinita de chaves fortes, que são sincronizadas pela rede. A conexão sem fio pode ser interrompida brevemente quando o roteador sem fio é reinicializado com a nova configuração da chave de segurança, mas isso costuma não ser detectado pelos usuários da rede.

Se nenhum computador estiver conectado à rede, a rotação de chaves ocorrerá depois que o primeiro se conectar.

Para ativar a rotação de chaves automática:

1 Clique com o botão direito do mouse no ícone do Wireless Network Security, na área de notificação do Windows.

2 Selecione **Exibir configuração**.

3 No painel Segurança da rede, marque **Ativar rotação de chaves automática**.

Você também retomar a rotação de chaves a partir do painel de Status da rede sem fio.

4 Clique em **Aplicar**.

Observação: A rotação de chaves ocorrerá automaticamente a cada 3 horas por padrão, mas você pode ajustar a freqüência da rotação de chaves de acordo com suas necessidades de segurança.

Tópicos relacionados

- Ajustar a freqüência da rotação de chaves (página 113)
- Continuar rotação de chaves (página 113)
- Exibir o número de rotações de chave (página 128)

Continuar rotação de chaves

Embora a rotação de chaves automática seja ativada por padrão, um computador com acesso administrativo pode retomar a rotação de chaves após suspendê-la.

Para retomar a rotação de chaves:

1. Clique com o botão direito do mouse no ícone do Wireless Network Security, na área de notificação do Windows.
2. Selecione **Exibir status**.
3. No painel de Status da rede sem fio, clique em **Continuar rotação de chaves**.

   Os alertas de Rotação de chaves iniciada e Chave de segurança trocada confirmam que a rotação de chaves foi iniciada e bem-sucedida.

Tópicos relacionados

- Rotação automática das chaves (página 112)
- Suspender a rotação de chaves automática (página 115)
- Exibir o número de rotações de chave (página 128)

Ajustar a freqüência da rotação de chaves

Se o Wireless Network Security estiver configurado para trocar automaticamente a chave de segurança da rede sem fio protegida, você poderá ajustar o período em que ocorrerá a rotação de chaves, variando desde a cada quinze minutos até a cada quinze dias

A McAfee recomenda que a chave de segurança seja trocada diariamente.

Para ajustar a freqüência da rotação de chaves automática:

1. Clique com o botão direito do mouse no ícone do Wireless Network Security, na área de notificação do Windows.
2. Selecione **Exibir configuração**.
3. No painel Segurança da rede, confirme se a rotação de chaves está ativada e mova o controle deslizante de **Freqüência** para uma das seguintes configurações:
   - **a cada 15 minutos**
   - **a cada 30 minutos**
   - **a cada 1 hora**
   - **a cada 3 horas**
   - **a cada 12 horas**

- **a cada 1 dia**
- **a cada 7 dias**
- **a cada 15 dias**

4 Clique em **Aplicar**.

Observação: Assegure-se de que a rotação de chaves automática esteja ativada antes de definir a freqüência da rotação de chaves.

Tópicos relacionados

- Ativar rotação de chaves automática (página 112)
- Exibir o número de rotações de chave (página 128)

Suspender a rotação de chaves automática

A rotação de chaves pode ser suspensa por qualquer computador conectado à rede sem fio. Você talvez deseje suspender a rotação de chaves por um dos seguintes motivos:

- Permitir que um visitante que não possua o Wireless Network Security instalado acesse a rede.
- Permitir que um sistema diferente do Windows, como Macintosh, Linux ou TiVo, tenha acesso. Depois de interromper a rotação de chaves, anote a chave e insira-a no novo dispositivo.
- Permitir uma conexão sem fio que não seja ininterrompida por rotações de chave para certos programas, como jogos on-line.
- Você deve retomar a rotação de chaves automática assim que possível para garantir que sua rede fique totalmente protegida contra hackers.

Para exibir a chave atual:

1. Clique com o botão direito do mouse no ícone do Wireless Network Security, na área de notificação do Windows.
2. Selecione **Exibir status**.
3. No painel Status da rede sem fio, sob o painel Rede sem fio protegida, clique em **Chave atual**. Anote a chave que aparece na caixa de diálogo Configuração da chave. Outros computadores que não têm o Wireless Network Security instalado podem utilizar essa chave para conectar à rede sem fio protegida.
4. Na caixa de diálogo Configuração da chave, clique em **Suspender rotação de chaves**.
5. Na caixa de diálogo Rotação de chaves suspensa, clique em **OK** para continuar a trabalhar.

Aviso: Se a rotação de chaves não for suspensa, dispositivos sem fio não suportados que estão conectados manualmente à rede serão desconectados quando ocorrer a rotação de chaves.

Você pode criar um disco Windows Connect Now e utilizar o arquivo de texto para copiar e colar a chave em outro computador e dispositivo.

Tópicos relacionados

- Ativar rotação de chaves automática (página 112)
- Adicionar computadores usando a tecnologia Windows Connect Now (página 91)
- Continuar rotação de chaves (página 113)

- Rotação automática das chaves (página 112)
- Exibir o número de rotações de chave (página 128)

Rotação manual de chaves de rede

O Wireless Network Security permite fazer a rotação de chaves manual, mesmo quando a rotação de chaves automática está ativada.

Para trocar manualmente uma chave da rede:

1. Clique com o botão direito do mouse no ícone do Wireless Network Security, na área de notificação do Windows.
2. Selecione **Exibir ferramentas**.
3. No painel Ferramentas, clique em **Ferramentas de manutenção**.
4. Na página Ferramentas de manutenção, em **Rotação manual da chave de segurança**, clique em **Girar**.

   O alerta de Rotação de chaves iniciada aparece e confirma que a rotação de chaves começou. Depois que a chave de segurança é trocada, o alerta de Chave de segurança trocada aparece, confirmando que a rotação de chaves foi bem-sucedida.

Observação: Para facilitar o gerenciamento de suas chaves de segurança, é possível ativar automaticamente a rotação de chaves no painel Segurança da rede.

Se nenhum computador estiver conectado à rede sem fio, a rotação de chaves ocorrerá automaticamente quando o primeiro se conectar.

Tópicos relacionados

- Ativar rotação de chaves automática (página 112)
- Ajustar a freqüência da rotação de chaves (página 113)
- Exibir o número de rotações de chave (página 128)

Exibir chaves como asteriscos

Por padrão, as chaves são exibidas como asteriscos, mas você pode configurar o Wireless Network Security para exibir as chaves em texto simples em redes que não são protegidas pelo Wireless Network Security.

Redes protegidas pelo Wireless Network Security exibem a chave em texto simples.

Para exibir chaves como asteriscos

1. Clique com o botão direito do mouse no ícone do Wireless Network Security na área de notificação do Windows.
2. Selecione **Exibir configuração**.
3. Clique em **Outras configurações**.
4. Desmarque a caixa **Exibir chaves em texto simples**.
5. Clique em **Aplicar**.

Tópicos relacionados

- Exibir chaves em texto simples (página 118)

Exibir chaves em texto simples

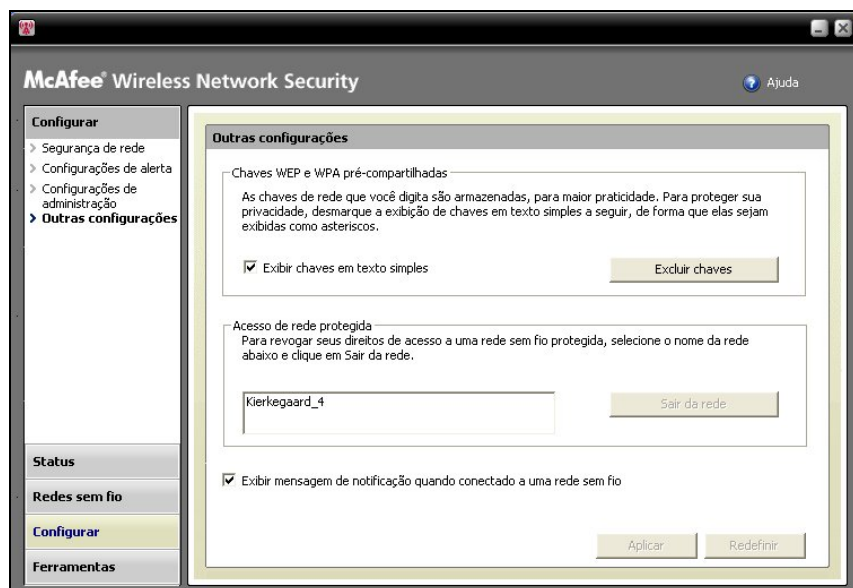
Por padrão, as chaves são exibidas como asteriscos, mas você pode configurar o Wireless Network Security para exibir as chaves em texto simples em redes que não são protegidas pelo Wireless Network Security.

Redes protegidas pelo Wireless Network Security exibem a chave em texto simples.

Para exibir chaves em texto simples:

1 Clique com o botão direito do mouse no ícone do Wireless Network Security na área de notificação do Windows.

2 Selecione **Exibir configuração**.

3 Clique em **Outras configurações**.

4 Marque a caixa **Exibir chaves em texto simples**.

5 Clique em **Aplicar**.

Tópicos relacionados

- Exibir chaves como asteriscos (página 117)

Excluir chaves de rede

O Wireless Network Security salva automaticamente suas chaves WEP e WPA pré-compartilhadas, que podem ser excluídas a qualquer momento.

Para excluir todas as chaves de sua rede:

1. Clique com o botão direito do mouse no ícone do Wireless Network Security na área de notificação do Windows.
2. Selecione **Exibir configuração**.
3. No painel **Configurar**, clique em **Outras configurações**.
4. No painel **Outras configurações**, em **Chaves WEP e WPA pré-compartilhadas**, clique em **Excluir chaves**.
5. Na caixa de diálogo Limpar chaves, clique em **Sim** se estiver seguro de que deseja excluir todas as chaves WEP e WPA pré-compartilhadas armazenadas.

Aviso: Quando excluídas, as chaves são removidas de forma permanente de seu computador. Depois de excluir suas chaves da rede, você deve inserir a chave correta para se conectar a uma rede WEP ou WPA.

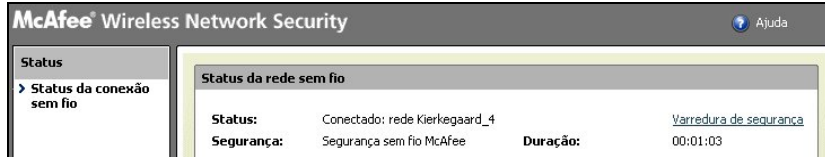
CAPÍTULO 17

Monitorando redes sem fio

O Wireless Network Security permite monitorar o status de sua rede sem fio e dos computadores protegidos.

Neste capítulo

Monitorando conexões de rede sem fio

Você pode exibir o status de sua conexão de rede, o modo de segurança, a velocidade, a duração, a intensidade de sinal e um relatório de segurança no painel Status da rede sem fio.

A tabela a seguir descreve os indicadores de status das conexões de rede sem fio.

Status	Descrição	Informações
Status	Indica se seu computador está conectado a uma rede e a qual rede ele está conectado	Exibir o status da conexão (página 123)
Segurança	Exibe o modo de segurança da rede a que você está conectado. O Wireless Network Security será exibido se você estiver protegido pelo Wireless Network Security.	Exibir o modo de segurança da rede (página 124)
Velocidade	Exibe a velocidade em que seu computador está conectado à rede.	Exibir a velocidade da conexão de rede (página 124)
Duração	Exibe o tempo de conexão do seu computador à rede.	Exibir a duração de sua conexão de rede (página 125)
Intensidade do sinal	Exibe a intensidade de sinal relativa da rede.	Exibir a intensidade do sinal da rede (página 126)
Varredura de segurança	Ao clicar em **Varredura de segurança** são exibidas informações de segurança, como vulnerabilidades da segurança sem fio, questões de desempenho e status de rede sem fio.	Exibir o relatório de segurança on-line (página 126)

Tópicos relacionados

- Sobre os ícones do Wireless Network Security (página 94)

Exibir o status da conexão

Você pode utilizar o painel Status da rede sem fio para rever o status da conexão da rede para confirmar se você está conectado ou desconectado da rede.

Para exibir o status da conexão sem fio:

1 Clique com o botão direito do mouse no ícone do Wireless Network Security na área de notificação do Windows.

2 Selecione **Exibir status**.

Os computadores conectados à rede sem fio protegida e a hora e a data em que cada um se conectou são exibidos no painel de Status da rede sem fio, em **Computadores.**

Tópicos relacionados

- Monitorando conexões de rede sem fio (página 122)
- Exibir o modo de segurança da rede (página 124)
- Exibir a velocidade da conexão de rede (página 124)
- Exibir a duração de sua conexão de rede (página 125)
- Exibir a intensidade do sinal da rede (página 126)
- Exibir o relatório de segurança on-line (página 126)

Exibir o modo de segurança da rede

Você pode utilizar o painel de Status da rede sem fio para exibir o modo de segurança da conexão de rede.

Para exibir o modo de segurança da rede:

1. Clique com o botão direito do mouse no ícone do Wireless Network Security na área de notificação do Windows.
2. Selecione **Exibir status**.

   O modo de segurança é exibido no painel Status da rede sem fio na caixa **Segurança**.

   O Wireless Network Security será exibido se a rede sem fio estiver protegida pelo Wireless Network Security.

Tópicos relacionados

- Monitorando conexões de rede sem fio (página 122)
- Exibir o status da conexão (página 123)
- Exibir a velocidade da conexão de rede (página 124)
- Exibir a duração de sua conexão de rede (página 125)
- Exibir a intensidade do sinal da rede (página 126)
- Exibir o relatório de segurança on-line (página 126)

Exibir a velocidade da conexão de rede

Você pode utilizar o painel Status da rede sem fio para exibir a velocidade da conexão de seu computador à rede.

Para exibir a velocidade da conexão de rede:

1. Clique com o botão direito do mouse no ícone do Wireless Network Security na área de notificação do Windows.
2. Selecione **Exibir status**.

   A velocidade da conexão é exibida no painel Status da rede sem fio na caixa **Velocidade**.

Tópicos relacionados

- Monitorando conexões de rede sem fio (página 122)
- Exibir o status da conexão (página 123)
- Exibir o modo de segurança da rede (página 124)
- Exibir a duração de sua conexão de rede (página 125)
- Exibir a intensidade do sinal da rede (página 126)
- Exibir o relatório de segurança on-line (página 126)

Exibir a duração de sua conexão de rede

Você pode utilizar o painel de Status da rede sem fio para exibir quanto tempo você ficou conectado à rede.

Para exibir a duração de sua conexão à rede:

1. Clique com o botão direito do mouse no ícone do Wireless Network Security na área de notificação do Windows.
2. Selecione **Exibir status**.

   O período em que seu computador esteve conectado à rede sem fio é exibido na caixa **Duração**.

Tópicos relacionados

- Monitorando conexões de rede sem fio (página 122)
- Exibir o status da conexão (página 123)
- Exibir o modo de segurança da rede (página 124)
- Exibir a velocidade da conexão de rede (página 124)
- Exibir a intensidade do sinal da rede (página 126)
- Exibir o relatório de segurança on-line (página 126)

Exibir a intensidade do sinal da rede

Você pode utilizar o painel Status da rede sem fio para exibir a intensidade de sinal da rede.

Para exibir a intensidade de sinal:

1. Clique com o botão direito do mouse no ícone do Wireless Network Security na área de notificação do Windows.
2. Selecione **Exibir status**.

   A qualidade do sinal é exibida na caixa **Intensidade do sinal**.

Tópicos relacionados

- Monitorando conexões de rede sem fio (página 122)
- Exibir o status da conexão (página 123)
- Exibir o modo de segurança da rede (página 124)
- Exibir a velocidade da conexão de rede (página 124)
- Exibir a duração de sua conexão de rede (página 125)
- Exibir o relatório de segurança on-line (página 126)

Exibir o relatório de segurança on-line

Você pode utilizar o painel Status da rede sem fio para exibir um relatório sobre sua conexão sem fio, esteja ela segura ou não.

A página da McAfee wi-fiscan exibe informações sobre as vulnerabilidades de sua segurança sem fio, questões de desempenho, informações sobre sua conexão sem fio, recomenda uma solução de segurança e indica se sua conexão está segura.

Antes de exibir o relatório de segurança, certifique-se de ter uma conexão com a Internet.

Para exibir um relatório de segurança on-line sobre sua rede:

1 Clique com o botão direito do mouse no ícone do Wireless Network Security na área de notificação do Windows.

2 Selecione **Exibir status**.

3 No painel Status da rede sem fio, clique em **Varredura de segurança**.

   Quando o navegador for aberto, você deverá fazer o download e instalar um componente ActiveX. Dependendo da configuração de seu navegador, ele pode bloquear o controle. Permita que seu navegador faça o download do componente e execute-o para começar a varredura. Dependendo da velocidade de conexão com a Internet, a varredura pode levar algum tempo.

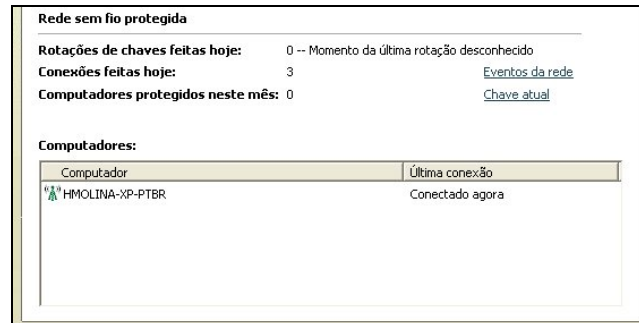
Observação: Consulte a documentação de seu navegador para obter informações sobre o download de componentes ActiveX.

O wi-fiscan da McAfee suporta o Internet Explorer 5.5 e posterior.

Tópicos relacionados

- Monitorando conexões de rede sem fio (página 122)
- Exibir o status da conexão (página 123)
- Exibir o modo de segurança da rede (página 124)
- Exibir a velocidade da conexão de rede (página 124)
- Exibir a duração de sua conexão de rede (página 125)
- Exibir a intensidade do sinal da rede (página 126)

Monitorando redes sem fio protegidas

O Wireless Network Security permite exibir o número de conexões, rotações de chaves e computadores protegidos no painel Status da rede sem fio. Você também pode exibir os eventos da rede, a chave atual e os computadores atualmente protegidos.

A tabela a seguir descreve os indicadores de status das conexões de rede sem fio protegidas

Status	Descrição	Informações
Rotações de chaves feitas hoje	Exibe o número diário de rotações de chaves na rede sem fio protegida.	Exibir o número de rotações de chave (página 128)
Conexões feitas hoje	Exibe o número diário de conexões à rede protegida.	Exibir o número de conexões diárias (página 129)
Computadores protegidos neste mês	Exibe o número de computadores protegidos no mês atual.	Exibir o número de computadores protegidos mensalmente (página 129)
Eventos da rede	Ao clicar em **Eventos da rede** são exibidos eventos da rede, conexão e rotação de chaves.	Exibir eventos da rede sem fio protegida (página 129)
Computadores	Exibe o número de computadores conectados à rede sem fio protegida e quando cada computador foi conectado.	Exibir computadores protegidos no momento (página 131)

Exibir o número de rotações de chave

Wireless Network Security permite exibir o número diário de rotações de chaves ocorridas na rede protegida, e quando a última rotação de chaves ocorreu.

Para exibir o número diário de rotações de chaves:

1. Clique com o botão direito do mouse no ícone do Wireless Network Security na área de notificação do Windows.
2. Selecione **Exibir status**.

   O número total de conexões e a rotação de chaves mais recente são exibidos no painel de Status da rede sem fio, sob **Rede sem fio protegida**, no campo **Rotações de chaves feitas hoje**.

Tópicos relacionados

- Monitorando redes sem fio protegidas (página 127)
- Exibir o número de conexões diárias (página 129)
- Exibir o número de computadores protegidos mensalmente (página 129)
- Exibir eventos da rede sem fio protegida (página 129)
- Exibir computadores protegidos no momento (página 131)
- Administrando chaves de rede (página 111)
- Rotação automática das chaves (página 112)
- Rotação manual de chaves de rede (página 116)

Exibir o número de conexões diárias

O Wireless Network Security permite exibir o número diário de conexões à rede protegida.

Para exibir as conexões de sua rede sem fio protegida:

1. Clique com o botão direito do mouse no ícone do Wireless Network Security na área de notificação do Windows.
2. Selecione **Exibir status**.

   O número total de conexões é exibido no painel de Status da rede sem fio, sob **Rede sem fio protegida**, na caixa **Conexões feitas hoje**.

Tópicos relacionados

- Monitorando redes sem fio protegidas (página 127)
- Exibir o número de computadores protegidos mensalmente (página 129)
- Exibir eventos da rede sem fio protegida (página 129)
- Exibir computadores protegidos no momento (página 131)

Exibir o número de computadores protegidos mensalmente

O Wireless Network Security permite exibir o número de computadores protegidos no mês atual.

Para exibir o número de computadores protegidos no mês atual:

1. Clique com o botão direito do mouse no ícone do Wireless Network Security na área de notificação do Windows.
2. Selecione **Exibir status**.
3. O número de computadores protegidos durante o mês atual é exibido no painel de Status da rede sem fio, em **Rede sem fio protegida**, na caixa **Computadores protegidos neste mês**.

Tópicos relacionados

- Monitorando redes sem fio protegidas (página 127)
- Exibir o número de rotações de chave (página 128)
- Exibir o número de conexões diárias (página 129)
- Exibir eventos da rede sem fio protegida (página 129)
- Exibir computadores protegidos no momento (página 131)

Exibir eventos da rede sem fio protegida

O Wireless Network Security registra eventos na rede sem fio, como quando as chaves de segurança são trocadas, quando outros computadores conectam à rede protegida pela McAfee e quando outros computadores entram na rede protegida pela McAfee.

O Wireless Network Security permite exibir um relatório que descreve eventos ocorridos em sua rede. Você pode especificar os tipos de eventos a serem exibidos e pode classificar as informações de acordo com data, evento ou computador.

Para exibir eventos da rede:

1 Clique com o botão direito do mouse no ícone do Wireless Network Security, na área de notificação do Windows.

2 Escolha uma das seguintes opções:

Para...	Faça isto...
Exibir eventos de rede a partir do painel Status da rede sem fio	1. Selecione **Exibir status**. 2. No painel de Status da rede sem fio, em **Rede sem fio protegida**, clique em **Eventos da rede**.
Exibir eventos de rede a partir do painel Status da rede sem fio	1. Clique em **Exibir ferramentas**. 2. No painel Ferramentas, clique em **Ferramentas de manutenção**. 3. No painel Ferramentas de manutenção, em **Exibir registros de eventos**, clique em **Exibir**.

3 Selecione um ou mais dos seguintes eventos a exibir:

- **Eventos da rede**: Exibe informações sobre a atividade da rede, como proteção de um roteador ou ponto de acesso sem fio.
- **Eventos de conexão**: Exibe informações sobre as conexões da rede, como a data e a hora em que um computador foi conectado à rede.
- **Eventos de rotação de chaves**: Exibe informações sobre as datas e as horas das rotações das chaves de segurança.

4 Clique em **Fechar**.

Tópicos relacionados

- Monitorando redes sem fio protegidas (página 127)
- Exibir o número de rotações de chave (página 128)
- Exibir o número de conexões diárias (página 128)
- Exibir o número de conexões diárias (página 129)
- Exibir computadores protegidos no momento (página 131)

Exibir computadores protegidos no momento

Você pode exibir o número de computadores conectados à rede sem fio protegida e quanto tempo cada computador ficou conectado.

Para exibir os computadores conectados à rede protegida:

1. Clique com o botão direito do mouse no ícone do Wireless Network Security na área de notificação do Windows.
2. Selecione **Exibir status**.
3. Computadores conectados à rede sem fio protegida, a hora e a data em que cada computador foi conectado mais recentemente, são exibidos no painel de Status da rede sem fio, em **Computadores.**

Tópicos relacionados

- Monitorando redes sem fio protegidas (página 127)
- Exibir o número de rotações de chave (página 128)
- Exibir o número de conexões diárias (página 128)
- Exibir o número de computadores protegidos mensalmente (página 129)
- Exibir eventos da rede sem fio protegida (página 129)

CAPÍTULO 18

Solução de problemas

Você pode diagnosticar os problemas ao utilizar o Wireless Security e um equipamento de terceiros, incluindo:

- Dificuldades na instalação
- Impossível proteger ou configurar sua rede
- Impossível conectar computadores à sua rede
- Impossível conectar-se a uma rede ou à Internet
- Outros problemas

Neste capítulo

Instalação do Wireless Network Security

Você pode diagnosticar os seguintes problemas de instalação.

- Em quais computadores instalar o software
- Adaptador sem fio não detectado
- Múltiplos adaptadores sem fio
- Não foi possível fazer download em computadores sem fio porque a rede já está segura

Em quais computadores instalar o software

Instale o Wireless Network Security em todos os computadores sem fio da sua rede (ao contrário de outros programas da McAfee, esse software pode ser instalado em vários computadores). Aceite o contrato de licença de aquisição do software. Em alguns casos, você pode precisar adquirir licenças adicionais.

É possível (mas não obrigatório) instalar em computadores que não tenham adaptadores sem fio, mas o software não estará ativo nesses computadores porque eles não precisam de proteção sem fio.

O Wireless Network Security é suportado atualmente no Windows XP ou no Windows 2000.

Adaptador sem fio compatível não detectado

Se o seu adaptador sem fio não for detectado ao ser instalado e ativado, reinicie o computador. Se o adaptador continuar não sendo detectado após o computador ser reiniciado, siga estas etapas.

1. Inicie a caixa de diálogo Propriedades de conexões de rede sem fio do Windows.
2. Utilizando o menu clássico do Windows, Iniciar, clique em **Iniciar**, aponte para **Configurações** e selecione **Conexões de rede**.
3. Clique no ícone **Conexão de rede sem fio**.
4. Na caixa de diálogo Conexão de rede sem fio, clique em **Propriedades**.
5. No painel de Propriedades da conexão de rede sem fio, desmarque **Filtro MWL** e, em seguida, marque-o novamente.

6. Clique em **OK**.

   Se isso não resolver o problema, verifique através da execução do WiFi Scan. Quando a varredura wi-fi funciona, significa que seu adaptador é suportado. Caso contrário, atualize o driver de seu adaptador (use a Atualização do Windows ou visite o site do fabricante na Web) ou adquira um novo dispositivo.

Tópicos relacionados

- Exibir o relatório de segurança on-line (página 126)

Múltiplos adaptadores sem fio

Se um erro informa que você tem múltiplos adaptadores sem fio instalados, você precisa desativar ou desconectar um deles. O Wireless Home Network Security funciona com apenas um adaptador sem fio.

Falha de download na rede protegida

Se você tem um CD de instalação, instale o Wireless Network Security a partir do CD em todos os computadores sem fio.

Caso tenha instalado o software em um computador sem fio e protegido a rede antes de instalar o software em todos os outros computadores sem fio, você tem as opções seguintes.

- Desproteja a rede. Em seguida, faça download do software e instale-o em todos os computadores sem fio. Proteja sua rede novamente.
- Visualize a chave de rede. Em seguida, digite a chave no seu computador sem fio para conectar-se à rede. Faça download do software, instale-o e associe-se à rede a partir do computador sem fio.
- Faça download do arquivo executável no computador que já está conectado à rede e salve-o em uma unidade flash USB ou grave-o em um CD para que você possa instalá-lo nos outros computadores.
- Execute a tecnologia Windows Connect Now.

Tópicos relacionados

- Remover roteadores ou pontos de acesso sem fio (página 101)
- Exibir chaves atuais (página 111)
- Adicionar computadores usando um dispositivo removível (página 89)
- Adicionar computadores usando a tecnologia Windows Connect Now (página 91)

Proteção ou configuração da sua rede

Você pode diagnosticar os seguintes problemas ao proteger ou configurar sua rede.

- Roteador ou ponto de acesso não suportado
- Atualizar o firmware do roteador ou ponto de acesso
- Erro de administrador duplicado
- A rede aparece insegura
- Não foi possível reparar

Roteador ou ponto de acesso não suportado

Se um erro informa que o roteador ou o ponto de acesso sem fio não são suportados, talvez o Wireless Network Security não consiga configurar o dispositivo por não tê-lo reconhecido ou encontrado.

Verifique se você tem a versão mais recente do Wireless Network Security solicitando uma atualização (a McAfee está constantemente acrescentando suporte para novos roteadores e pontos de acesso). Se o seu roteador ou ponto de acesso aparece na lista de roteadores suportados e esse erro ainda ocorre, você está com problemas de comunicação entre o computador e o roteador ou ponto de acesso.

Tópicos relacionados

- Roteadores sem fio suportados
  http://www.mcafee.com/router

Atualizar o firmware do roteador ou ponto de acesso

Se um erro informa que a revisão do firmware do seu roteador ou ponto de acesso sem fio não é suportada, isso significa que o seu dispositivo é suportado, mas a revisão do firmware do dispositivo não é. Verifique se você tem a versão mais recente do Wireless Network Security solicitando uma atualização (a McAfee está constantemente acrescentando suporte para novas revisões de firmware).

Se você tiver a versão mais recente do Wireless Network Security, consulte o site ou organização de suporte do fabricante do seu roteador ou ponto de acesso e instale uma versão de firmware que esteja relacionada na lista de roteadores suportados.

Tópicos relacionados

- Roteadores sem fio suportados
  http://www.mcafee.com/router

Erro de administrador duplicado

Após configurar o seu roteador ou ponto de acesso, você precisa efetuar logoff na interface de administração. Em alguns casos, se você não efetuar logoff, o roteador ou o ponto de acesso atuará como se um outro computador ainda o estivesse configurando e uma mensagem de erro aparecerá.

Se não puder efetuar logoff, desconecte a alimentação do roteador ou do ponto de acesso e, em seguida, conecte-a novamente.

Falha na rotação de chaves

A rotação de chaves falhou porque:

- As informações de logon para o seu roteador ou ponto de acesso foram alteradas.
- A versão do firmware do seu roteador ou ponto de acesso foi alterada para uma versão não suportada.
- O seu roteador ou ponto de acesso não está disponível. Verifique se o roteador ou o ponto de acesso está ligado e se está conectado à sua rede.
- Erro de administrador duplicado.
- Em alguns roteadores sem fio, se outro computador for registrado manualmente na interface da Web do roteador sem fio, é possível que o cliente McAfee também não consiga acessar a interface de gerenciamento para fazer a rotação de chaves da criptografia.

Tópicos relacionados

- Alterar as credenciais para dispositivos sem fio (página 109)
- Rotação automática das chaves (página 112)

Impossível reparar o roteador ou ponto de acesso

Se o reparo falhar, tente o seguinte. Observe que cada procedimento é independente.

- Conecte-se à sua rede utilizando um cabo e, em seguida, tente reparar novamente.
- Desligue a alimentação do roteador ou do ponto de acesso, ligue-a novamente e experimente conectar.
- Redefina o roteador ou o ponto de acesso sem fio com sua configuração padrão e repare-o. Essa ação redefine as configurações sem fio para as originais. Em seguida, redefina as configurações de sua conexão com a Internet.
- Utilizando as opções avançadas, saia da rede em todos os computadores, redefina o roteador ou o ponto de acesso sem fio com suas configurações padrão e, em seguida, proteja a rede. Essa ação redefine as configurações sem fio para as originais. Em seguida, redefina as configurações de sua conexão com a Internet.

Tópicos relacionados

- Reparar configurações de segurança da rede (página 110)

A rede parece desprotegida

Se a sua rede aparece como insegura, ela não está protegida. É necessário proteger a rede para torná-la segura. Observe que o Wireless Network Security somente funciona com roteadores e pontos de acesso compatíveis.

Tópicos relacionados

- Criar redes sem fio protegidas (página 80)
- Roteadores sem fio suportados http://www.mcafee.com/router

Conexão de computadores à sua rede

Você pode diagnosticar os seguintes problemas ao conectar computadores à sua rede.

- Aguardando autorização
- Concessão de acesso a um computador desconhecido

Aguardando autorização

Se você tentar se associar a uma rede protegida e o seu computador permanecer aguardando autorização, verifique o seguinte.

- Se um computador sem fio que já tenha acesso à rede está ligado e conectado à rede.
- Se há alguém presente para conceder acesso nesse computador quando ele aparece.
- Se os computadores se encontram dentro do alcance um do outro.

Se **Conceder acesso** não aparecer no computador que já tem acesso à rede, experimente conceder a partir de um outro computador.

Se não houver outros computadores disponíveis, desproteja a rede a partir do computador que já tem acesso e proteja a rede a partir do computador que não tinha acesso. Em seguida, associe-se à rede a partir do computador que protegeu a rede originalmente.

Você também pode utilizar o recurso Proteger outro computador.

Tópicos relacionados

- Associar-se a uma rede sem fio protegida (página 82)
- Sair de redes sem fio protegidas (página 104)
- Remover roteadores ou pontos de acesso sem fio (página 101)
- Adicionar computadores à rede sem fio protegida (página 89)

Concessão de acesso a um computador desconhecido

Quando receber um pedido de um computador desconhecido para conceder acesso, negue-o até poder verificar sua legitimidade. Alguém pode estar tentando um acesso ilegítimo à sua rede.

Conectando à Internet e à rede

Você pode diagnosticar os seguintes problemas ao conectar a uma rede ou à Internet.

- Conexão deficiente com a Internet
- A conexão pára por alguns instantes
- Dispositivos (que não o computador) perdem a conexão
- Solicitação para digitar a chave WEP, WPA ou WPA2
- Não foi possível conectar
- Atualize seu adaptador sem fio
- Nível de sinal fraco
- O Windows não pôde configurar a sua conexão sem fio
- O Windows mostra que não há conexão

Não é possível conectar à Internet

Se não conseguir se conectar, experimente acessar a sua rede utilizando um cabo e, em seguida, conecte-se à Internet. Se ainda assim não conseguir, verifique se:

- Seu modem está ligado
- Suas configurações PPPoE estão corretas
- Sua linha DSL ou de cabo está ativa

Problemas de conectividade, como velocidade e intensidade do sinal, também podem ser causados por interferência de equipamentos sem fio. Tente os seguintes métodos para corrigir o problema.

- Mude o canal de seu telefone sem fio
- *Elimine as possíveis fontes de interferência
- Mude o local de seu roteador, ponto de acesso sem fio ou computador
- Mude o canal do roteador ou ponto de acesso. Canais 1, 4, 7 e 11 são recomendados para América do Norte e América do Sul. Canais 1, 4, 7, 13 são recomendados para outros países. Muitos roteadores estão definidos para o canal 6 por padrão
- Certifique-se de que seu roteador e adapatador sem fio (especialmente um adaptador USB sem fio) não estejam contra uma parede
- Certifique-se de que seu adaptador sem fio USB não esteja ao lado de um PA/roteador sem fio
- Posicione o roteador longe de paredes e metais

Conexão interrompida

Quando sua conexão é interrompida por alguns instantes (por exemplo, durante um jogo on-line), a rotação de chaves pode ser a causa. Para evitar isso, você pode suspender a rotação de chaves.

A McAfee recomenda retomar a rotação de chaves assim que possível para garantir que a rede fique totalmente protegida contra hackers.

Tópicos relacionados

- Rotação automática das chaves (página 112)
- Continuar rotação de chaves (página 113)
- Suspender a rotação de chaves automática (página 115)
- Rotação manual de chaves de rede (página 116)

Dispositivos perdem a conectividade

Se alguns dispositivos estão perdendo a conexão quando você utiliza o Wireless Network Security, tente corrigir o problema usando os seguintes métodos:

- Suspender a rotação de chaves
- Atualizar o driver do adaptador sem fio
- Desativar o gerenciador cliente do adaptador

Tópicos relacionados

- Suspender a rotação de chaves automática (página 115)

Solicitação para digitar a chave WEP, WPA ou WPA2

Se for necessário digitar uma chave WEP, WPA ou WPA2 para se conectar à sua rede sem fio protegida, você provavelmente não instalou o software no seu computador.

Para funcionar corretamente, o Wireless Network Security precisa estar instalado em todos os computadores sem fio da sua rede.

Tópicos relacionados

- Iniciando o Wireless Network Security (página 74)
- Adicionar computadores à rede sem fio protegida (página 89)

Impossível conectar à rede sem fio

Se não conseguir se conectar, experimente o seguinte. Observe que cada procedimento é independente.

- Se não estiver se conectando a uma rede protegida, verifique se você tem a chave correta e digite-a novamente.
- Desconecte o adaptador sem fio e conecte-o novamente ou desative-o e reative-o.
- Desligue o roteador ou o ponto de acesso, ligue-o novamente e, em seguida, tente conectar.
- Verifique se o seu roteador ou ponto de acesso sem fio está conectado e repare as configurações de segurança.
- Reinicie o computador.
- Atualize o adaptador sem fio ou compre um novo. Por exemplo, a sua rede pode estar usando segurança WPA-PSK TKIP e talvez o seu adaptador sem fio não suporte o modo de segurança da rede (as redes mostram WEP, muito embora estejam definidas como WPA).
- Se não puder se conectar após atualizar o roteador ou o ponto de acesso sem fio, talvez você o tenha atualizado para uma versão não suportada. Verifique se o roteador ou o ponto de acesso é suportado. Se a versão não for suportada, remova a atualização para voltar a uma versão suportada ou espere até que uma atualização do Wireless Security esteja disponível.

Tópicos relacionados

- Reparar configurações de segurança da rede (página 110)
- Atualização do seu adaptador sem fio (página 143)

Atualize seu adaptador sem fio

Pode ser necessário atualizar seu adaptador sem fio para que você possa utilizar o Wireless Network Security.

Para atualizar o seu adaptador:

1. Na área de trabalho, clique em **Iniciar**, aponte para **Configurações** e, em seguida, selecione **Painel de controle**.
2. Clique duas vezes no ícone **Sistema**. A caixa de diálogo **Propriedades do sistema** aparece.
3. Selecione a guia **Hardware** e, em seguida, clique em **Gerenciador de dispositivos**.
4. Na lista Gerenciador de dispositivos, clique duas vezes no seu adaptador.
5. Selecione a guia **Driver** e anote o driver que você possui.
6. Visite o site do fabricante do adaptador na Web para localizar uma atualização. Os drivers costumam ser encontrados na seção Suporte ou Downloads. Se você estiver utilizando uma

placa miniPCI, navegue até o fabricante do computador e não da placa.

7. Se houver uma atualização de driver disponível, siga as instruções do site para fazer download.
8. Volte para a guia **Driver** e clique em **Atualizar driver**. Um assistente do Windows aparecerá.
9. Para instalar o driver, siga as instruções no site da Web.

Nível de sinal fraco

Se a sua conexão cair ou estiver lenta, talvez o nível do sinal não esteja suficientemente forte. Para melhorar o sinal, tente o seguinte:

- Verifique se os seus dispositivos sem fio não estão sendo bloqueados por objetos metálicos, como aquecedores, dutos ou aparelhos volumosos. Os sinais sem fio não se propagam bem através desses objetos.
- Se o seu sinal atravessa paredes, certifique-se de que ele não tenha de fazê-lo em um ângulo muito raso. Quanto maior o espaço percorrido pelo sinal dentro da parede, mais fraco ele fica.
- Se o seu roteador ou ponto de acesso sem fio possui mais de uma antena, experimente orientar ambas as antenas perpendicularmente entre si (por exemplo, uma na vertical e outra na horizontal, em um ângulo de 90 graus).
- Alguns fabricantes produzem antenas de alto ganho. Antenas direcionais proporcionam maior alcance, enquanto antenas onidirecionais oferecem maior versatilidade. Consulte as instruções de instalação do fabricante para instalar a antena.

Se essas etapas não forem bem-sucedidas, adicione à sua rede um ponto de acesso que esteja mais perto do computador ao qual você está tentando se conectar. Se você configurar o seu segundo ponto de acesso com o mesmo nome de rede (SSID) e um canal diferente, o seu adaptador encontrará automaticamente o sinal mais forte e fará a conexão através do ponto de acesso apropriado.

Tópicos relacionados

- Ícones de intensidade do sinal (página 95)
- Exibir a intensidade do sinal da rede (página 125)

O Windows não suporta conexão sem fio

Se uma mensagem de erro do Windows indicar que ele não pode configurar a sua conexão sem fio, você poderá ignorar isso. Use o Wireless Network Security para conectar e configurar redes sem fio.

Na caixa de diálogo Propriedades de conexões de rede sem fio do Windows, sob a guia Redes sem fio, verifique se a caixa **Usar o Windows para definir minhas configurações de rede sem fio** está desmarcada.

O Wireless Network Security permite:

- Adaptadores instalados em computadores que executam Windows 2000 podem se conectar a redes WPA, mesmo se o gerenciador cliente da placa não for suportado.
- Adaptadores em computadores que executam Windows XP podem se conectar a redes WPA2 sem precisar localizar e instalar o Win XP SP2 hotfix.
- Adaptadores sob Windows XP SP1 podem ser conectar a redes WPA e WPA2 sem precisar localizar e instalar um hotfix, que não é suportado pelo Windows XP SP1.

O Windows mostra que não há conexão

Se você estiver conectado, mas o ícone de rede do Windows estiver mostrando um X (sem conexão), ignore isso. A sua conexão está boa.

Outros problemas

Você pode diagnosticar os seguintes problemas:

- Nome de rede diferente ao utilizar outros programas
- Problema quando configuro roteadores ou pontos de acesso sem fio
- Substituir computadores
- Selecionar outro modo de segurança
- Software não funciona após atualização de sistema operacional

O nome de rede fica diferente ao utilizar outros programas

Se o nome da rede for diferente ao ser visualizado através de outros programas (por exemplo, tendo _SafeAaf como parte do nome), isso é normal.

O Wireless Network Security marca as redes com um código quando elas são protegidas.

Configurar roteadores ou pontos de acesso sem fio

Se aparecer um erro ao configurar o seu roteador ou ponto de acesso ou ao adicionar múltiplos roteadores na rede, verifique se cada roteador e ponto de acesso possui um endereço IP distinto.

Se o nome do seu roteador ou ponto de acesso sem fio aparece na caixa de diálogo Proteger roteador ou ponto de acesso sem fio, mas ocorre um erro quando você o configura: Verifique se há suporte para o seu roteador ou ponto de acesso.

Se o seu roteador ou ponto de acesso está configurado, mas não parece estar na rede correta (por exemplo, se não é possível ver os outros computadores ligados à LAN), verifique se você configurou o o roteador ou ponto de acesso apropriado, e não o de seu vizinho. Desconecte a alimentação do roteador ou do ponto de acesso e verifique se a conexão cai. Se o roteador ou o ponto de acesso errado for configurado, desproteja-o e, em seguida, proteja o roteador ou o ponto de acesso certo.

Se você não consegue configurar ou adicionar o seu roteador ou ponto de acesso, havendo suporte para o mesmo, algumas alterações feitas por você podem estar impedindo-o de ser configurado corretamente.

- Siga as instruções do fabricante para configurar o seu roteador ou ponto de acesso sem fio para DHCP ou para configurar o endereço IP correto. Em alguns casos, o fabricante fornece uma ferramenta de configuração.
- Redefina o seu roteador ou ponto de acesso com os padrões de fábrica e tente reparar a sua rede novamente. Você pode ter alterado a porta de administração no roteador ou ponto de acesso ou desativado a administração sem fio. Verifique se você está usando a configuração padrão e se a configuração sem fio está ativada. Uma outra possibilidade é a administração http estar desativada. Nesse caso, verifique se a administração http está ativada. Certifique-se de utilizar a porta 80 para administração.
- Se o seu roteador ou ponto de acesso sem fio não aparece na lista de roteadores ou pontos de acesso sem fio a serem protegidos ou conectados, ative a difusão de SSID e verifique se o seu roteador ou ponto de acesso está presente na lista de redes sem fio disponíveis do Wireless Network Security.
- Se você for desconectado ou não puder estabelecer uma conexão, a filtragem de MAC poderá estar ativada. Desative a filtragem de MAC.
- Caso não consiga executar operações de rede (por exemplo, compartilhar arquivos ou imprimir em impressoras compartilhadas) entre dois computadores com conexão sem fio à rede, verifique se você não ativou o “AP Isolation”. Esse recurso impede que computadores sem fio se conectem uns aos outros através da rede.

- Se você está utilizando um programa de firewall diferente do McAfee Personal Firewall, certifique-se de que a sub-rede seja confiável.

Tópicos relacionados

- Roteadores sem fio suportados http://www.mcafee.com/router

Substituir computadores

Se o computador que protegia a rede foi substituído e não há computador algum que tenha acesso (ou seja, se você não consegue acessar a rede), redefina o roteador ou o ponto de acesso sem fio com seus padrões de fábrica e proteja a rede novamente.

Selecionar outro modo de segurança

Se um erro informar que você selecionou um modo de segurança que não é suportado pelo adaptador sem fio, será necessário selecionar um modo de segurança diferente.

- Todos os adaptadores suportam WEP.
- A maioria dos adaptadores que suportam WPA implementam os dois modos de segurança, WPA-PSK TKIP e WPA-PSK AES.
- Adaptadores que suportam WPA2 implementam modos de segurança WPA e WPA2-PSK TKIP, WPA2-PSK AES e WPA2-PSK TKIP/AES.

Tópicos relacionados

- Definição de configurações de segurança (página 106)
- Exibir o modo de segurança da rede (página 124)

O software falha após o upgrade dos sistemas operacionais

Se o Wireless Network Security falhar após o upgrade dos sistemas operacionais, remova e em seguida reinstale o programa.

CAPÍTULO 19

McAfee EasyNetwork

O McAfee® EasyNetwork ativa o compartilhamento seguro de arquivos, simplifica as transferências de arquivos e automatiza o compartilhamento de impressoras entre computadores de sua rede doméstica.

Antes de começar a usar o EasyNetwork, você pode se familiarizar com alguns dos recursos mais populares. A Ajuda do Easynetwork fornece detalhes sobre como configurar e usar esses recursos.

Neste capítulo

Recursos

O EasyNetwork fornece os recursos a seguir.

Compartilhamento de arquivos

O EasyNetwork facilita o compartilhamento de arquivos entre seu computador e os outros computadores da rede. Ao compartilhar arquivos, você concede aos outros computadores acesso somente leitura a esses arquivos. Apenas computadores membros da rede gerenciada (isto é, com acesso total ou administrativo) podem compartilhar arquivos ou acessar arquivos compartilhados por outros membros.

Transferência de arquivos

É possível enviar arquivos a outros computadores que sejam membros da rede gerenciada. Quando você recebe um arquivo, ele aparece em sua caixa de entrada do EasyNetwork. A caixa de entrada é um local de armazenamento temporário para todos os arquivos enviados para você por outros computadores da rede.

Compartilhamento automático de impressoras

Depois que você se associa à rede gerenciada, o EasyNetwork compartilha automaticamente todas as impressoras locais conectadas ao seu computador, usando o nome atual da impressora como nome da impressora compartilhada. Ele também detecta impressoras compartilhadas por outros computadores em sua rede e permite que você configure e use essas impressoras.

CAPÍTULO 20

Configurando o EasyNetwork

Antes de usar os recursos do EasyNetwork, você deve iniciar o programa e associar-se à rede gerenciada. Depois de associar-se, você pode decidir sair da rede a qualquer momento.

Neste capítulo

Iniciando o EasyNetwork

Por padrão, você é solicitado a iniciar o EasyNetwork imediatamente depois da instalação; no entanto, você também pode iniciar o EasyNetwork mais tarde.

Iniciar o EasyNetwork

Por padrão, você é solicitado a iniciar o EasyNetwork imediatamente depois da instalação; no entanto, você também pode iniciar o EasyNetwork mais tarde.

Para iniciar o EasyNetwork:

- No menu **Iniciar**, aponte para **Programas**, aponte para **McAfee** e clique em **McAfee EasyNetwork**.

Dica: Se você aceitou criar ícones na área de trabalho e na inicialização rápida durante a instalação, também é possível iniciar o EasyNetwork clicando duas vezes no ícone do McAfee EasyNetwork na área de trabalho ou clicando no ícone do McAfee EasyNetwork na área de notificação à direita da barra de tarefas.

Associando-se a uma rede gerenciada

Depois de instalar o SecurityCenter, um agente de rede é adicionado ao computador e executado em segundo plano. No EasyNetwork, o agente de rede é responsável por detectar uma conexão de rede válida, detectando impressoras locais a serem compartilhadas e monitorando o status da rede.

Se na rede à qual você estiver conectado no momento não for encontrado nenhum outro computador que execute o agente de rede, você será automaticamente transformado em membro da rede e solicitado a identificar se a rede é confiável. Por ser o primeiro computador a associar-se à rede, o nome do seu computador é incluído no nome da rede, mas você poderá renomeá-la quando desejar.

Quando um computador se conecta à rede, uma solicitação de associação é enviada a todos os outros computadores atualmente na rede. A solicitação pode ser concedida por qualquer outro computador com permissões administrativas da rede. O concessor também pode determinar o nível de permissão para o computador que está se associando à rede no momento; por exemplo, convidado (apenas capacidade de transferência de arquivos) ou total/administrativa (capacidade para transferência e compartilhamento de arquivos). No EasyNetwork, computadores com acesso administrativo podem conceder acesso a outros computadores e gerenciar permissões (isto é, promover ou rebaixar computadores); computadores com acesso total não podem executar essas tarefas administrativas. Antes de permitir a associação do computador, é realizado um teste de segurança.

Observação: Depois da associação, se você tiver outros programas de rede da McAfee instalados (o McAfee Wireless Network Security ou o Network Manager, por exemplo), o computador também será reconhecido como membro gerenciado nesses programas. O nível de permissão atribuído a um computador aplica-se a todos os programas de rede da McAfee. Para obter mais informações sobre o que significam permissões de convidado, total ou administrativa em outros programas de rede da McAfee, consulte a documentação fornecida com o programa.

Associar-se à rede

Quando um computador se conecta a uma rede confiável pela primeira vez depois da instalação do EasyNetwork, uma mensagem pergunta se você deseja se associar à rede gerenciada. Quando o computador concorda em associar-se, uma solicitação é enviada a todos os outros computadores da rede que têm acesso administrativo. Essa solicitação deve ser concedida para que o computador possa compartilhar impressoras e arquivos ou enviar e copiar arquivos da rede. Se o computador for o primeiro computador na rede, ele recebe permissões administrativas automaticamente.

Para associar-se à rede:

1 Na janela Arquivos compartilhados, clique em **Sim, associar à rede agora**.
Quando um computador administrador da rede autorizar sua solicitação, aparecerá uma mensagem perguntando se você deseja permitir que esse computador e os outros computadores da rede gerenciem as configurações de segurança uns dos outros.

2 Para permitir que seu computador e os outros da rede gerenciem as configurações de segurança uns dos outros, clique em **Sim**; caso contrário, clique em **Não**.

3 Confirme se o computador concessor está exibindo as mesmas cartas de baralho que estão sendo exibidas na caixa de diálogo de confirmação de segurança e clique em **Confirmar**.

Observação: Se o computador concessor não exibir as mesmas cartas que são exibidas na caixa de diálogo de confirmação de segurança, houve uma violação de segurança na rede gerenciada. Associar-se à rede poderia colocar seu computador em risco, portanto, clique em **Rejeitar** na caixa de diálogo de confirmação de segurança.

Conceder acesso à rede

Quando um computador solicita associar-se à rede gerenciada, uma mensagem é enviada aos outros computadores da rede que têm acesso administrativo. O primeiro computador a responder à mensagem torna-se o concessor. Como concessor, você é responsável por decidir que tipo de acesso deve ser concedido ao computador: convidado, total ou administrativo.

Para conceder acesso à rede:

1 No alerta, marque uma das caixas de seleção a seguir:

- **Conceder acesso convidado**: Permite que o usuário envie arquivos a outros computadores, mas não compartilhe arquivos.

- **Conceder acesso total para todos os aplicativos gerenciados da rede gerenciada**: Permite que o usuário envie e compartilhe arquivos.
- **Conceder acesso administrativo para todos os aplicativos da rede gerenciada**: Permite que o usuário envie e compartilhe arquivos, conceda acesso a outros computadores e ajuste o nível de permissão de outros computadores.

2. Clique em **Conceder acesso**.
3. Confirme se o computador está exibindo as mesmas cartas de baralho que estão sendo exibidas na caixa de diálogo de confirmação de segurança e clique em **Confirmar**.

Observação: Se o computador não exibir as mesmas cartas que estão sendo exibidas na caixa de diálogo de confirmação de segurança, houve uma violação de segurança na rede gerenciada. Conceder acesso à rede para esse computador pode colocar seu computador em risco, portanto, clique em **Rejeitar** na caixa de diálogo de confirmação de segurança.

Renomear a rede

Por padrão, o nome da rede inclui o nome do primeiro computador associado, mas você pode mudar o nome da rede a qualquer momento. Ao renomear a rede, você muda a descrição dela exibida no EasyNetwork.

Para renomear a rede:

1. No menu **Opções**, clique em **Configurar**.
2. Na caixa de diálogo Configurar, digite o nome da rede na caixa **Nome da rede**.
3. Clique em **OK**.

Saindo de uma rede gerenciada

Se você se associar a uma rede gerenciada e depois decidir que não quer mais ser um membro, é possível deixar a rede. Depois de renunciar à sua associação, você pode se associar novamente a qualquer momento, mas será preciso receber permissão para associar-se e executar a verificação de segurança novamente. Para obter mais informações, consulte Associando-se a uma rede gerenciada (página 153).

Sair de uma rede gerenciada

Você pode sair da rede gerenciada à qual se associou anteriormente.

Para sair de uma rede gerenciada:

1. No menu **Ferramentas**, clique em **Sair da rede**.
2. Na caixa de diálogo Sair da rede, selecione o nome da rede da qual deseja sair.
3. Clique em **Sair da rede**.

CAPÍTULO 21

Compartilhando e enviando arquivos

O EasyNetwork facilita o compartilhamento e o envio de arquivos entre seu computador e os outros computadores da rede. Ao compartilhar arquivos, você concede aos outros computadores acesso somente leitura a esses arquivos. Apenas computadores membros da rede gerenciada (isto é, com acesso total ou administrativo) podem compartilhar arquivos ou acessar arquivos compartilhados por outros computadores-membros.

Neste capítulo

Compartilhando arquivos

O EasyNetwork facilita o compartilhamento de arquivos entre seu computador e os outros computadores da rede. Ao compartilhar arquivos, você concede aos outros computadores acesso somente leitura a esses arquivos. Apenas computadores membros da rede gerenciada (isto é, com acesso total ou administrativo) podem compartilhar arquivos ou acessar arquivos compartilhados por outros computadores-membros. Se você compartilhar uma pasta, todos os arquivos da pasta e suas subpastas serão compartilhados, mas arquivos adicionados posteriormente à pasta não serão compartilhados automaticamente. Se uma pasta ou um arquivo compartilhado for excluído, será imediatamente removido da janela Arquivos compartilhados. É possível parar de compartilhar arquivos a qualquer momento.

Você pode acessar arquivos compartilhados de duas maneiras: abrindo o arquivo diretamente a partir do EasyNetwork ou copiando o arquivo para um local em seu computador e abrindo-o em seguida. Se sua lista de arquivos compartilhados ficar longa, você poderá procurar os arquivos compartilhados que deseja acessar.

Observação: Arquivos compartilhados através do EasyNetwork não podem ser acessados a partir de outros computadores por meio do Windows Explorer. O compartilhamento de arquivos do EasyNetwork é realizado em conexões seguras.

Compartilhar um arquivo

Quando você compartilha um arquivo, ele se torna automaticamente disponível para todos os outros membros com acesso total ou administrativo à rede gerenciada.

Para compartilhar um arquivo:

1. No Windows Explorer, localize o arquivo que deseja compartilhar.
2. Arraste o arquivo de seu local no Windows Explorer até a janela Arquivos compartilhados no EasyNetwork.

Dica: Você também pode compartilhar um arquivo clicando em **Compartilhar arquivos** no menu **Ferramentas**. Na caixa de diálogo Compartilhar, navegue até a pasta em que está armazenado o arquivo que deseja compartilhar e clique em **Compartilhar**.

Parar de compartilhar um arquivo

Se você compartilhar um arquivo na rede gerenciada, poderá parar de compartilhá-lo a qualquer momento. Quando você para de compartilhar um arquivo, os outros membros da rede gerenciada não podem mais acessá-lo.

Para parar de compartilhar um arquivo:

1 No menu **Ferramentas**, clique em **Deixar de compartilhar arquivos**.
2 Na caixa de diálogo Deixar de compartilhar arquivos, selecione o arquivo que não deseja mais compartilhar.
3 Clique em **Não compartilhar**.

Copiar um arquivo compartilhado

Você pode copiar arquivos compartilhados de qualquer computador da rede gerenciada para o seu computador. Depois, se o computador parar de compartilhar o arquivo, você ainda terá uma cópia.

Para copiar um arquivo:

- Arraste um arquivo da janela Arquivos compartilhados do EasyNetwork para um local no Windows Explorer ou para a área de trabalho do Windows.

Dica: Você também pode copiar um arquivo compartilhado selecionando o arquivo no EasyNetwork e clicando em **Copiar para** no menu **Ferramentas**. Na caixa de diálogo Copiar para, navegue até a pasta para a qual deseja copiar o arquivo, selecione-a e clique em **Salvar**.

Procurar um arquivo compartilhado

Você pode procurar um arquivo que foi compartilhado por você ou por qualquer outro membro da rede. Enquanto você digita os critérios de pesquisa, o EasyNetwork exibe automaticamente os resultados correspondentes na janela Arquivos compartilhados.

Para procurar um arquivo compartilhado:

1 Na janela Arquivos compartilhados, clique em **Pesquisar**.
2 Clique em uma das opções a seguir, na lista **Contém**:
   - **Contém todas as palavras**: Procura todos os nomes de arquivos ou caminhos que contenham todas as palavras especificadas na lista **Nome do arquivo ou caminho**, em qualquer ordem.

- **Contém qualquer uma das palavras**: Pesquisa nomes de arquivos ou caminhos que contenham qualquer uma das palavras especificadas na lista **Nome do arquivo ou caminho**.
- **Contém a seqüência de caracteres exata**: Procura nomes de arquivos ou caminhos que contenham a frase exata especificada na lista **Nome do arquivo ou caminho**.

3 Digite uma parte ou todo o nome do arquivo ou caminho na lista **Nome do arquivo ou caminho**.

4 Clique em um dos tipos de arquivos a seguir, na lista **Tipo**:

- **Qualquer**: Pesquisa todos os tipos de arquivos compartilhados.
- **Documento**: Pesquisa todos os documentos compartilhados.
- **Imagem**: Pesquisa todos os arquivos de imagem compartilhados.
- **Vídeo**: Pesquisa todos os arquivos de vídeo compartilhados.
- **Áudio**: Pesquisa todos os arquivos de áudio compartilhados.

5 Nas listas **De** e **Até**, clique em datas que representem o intervalo de datas durante o qual o arquivo foi criado.

Enviando arquivos para outros computadores

É possível enviar arquivos a outros computadores que sejam membros da rede gerenciada. Antes de enviar um arquivo, o EasyNetwork confirma se o computador de destino tem espaço em disco disponível suficiente.

Quando você recebe um arquivo, ele aparece em sua caixa de entrada do EasyNetwork. A caixa de entrada é um local de armazenamento temporário para todos os arquivos enviados para você por outros computadores da rede. Se o EasyNetwork estiver aberto no momento em que você recebe um arquivo, o arquivo aparece instantaneamente em sua caixa de entrada. Caso contrário, aparecerá uma mensagem na área de notificação à direita da barra de tarefas do Windows. Se não desejar receber mensagens de notificação, você pode desligá-las. Se um arquivo com o mesmo nome já existir na caixa de entrada, o novo arquivo é renomeado com um sufixo numérico. Os arquivos permanecem em sua caixa de entrada até que você os aceite (isto é, copie-os para um local em seu computador).

Enviar um arquivo para outro computador

Você pode enviar um arquivo diretamente para outro computador na rede gerenciada, sem compartilhá-lo. Para que um usuário no computador de destino possa exibir o arquivo, este deve ser salvo localmente. Para obter mais informações, consulte Aceitar um arquivo de outro computador (página 164).

Para enviar um arquivo para outro computador:

1. No Windows Explorer, localize o arquivo que deseja enviar.
2. Arraste o arquivo de seu local no Windows Explorer até um ícone de um computador ativo no EasyNetwork.

Dica: Você pode enviar diversos arquivos para um computador, pressionando CTRL ao selecionar os arquivos. Também é possível enviar os arquivos clicando em **Enviar** no menu **Ferramentas**, selecionando os arquivos e, em seguida, clicando em **Enviar**.

Aceitar um arquivo de outro computador

Se outro computador da rede gerenciada enviar um arquivo para você, você deverá aceitá-lo (salvando-o em uma pasta do seu computador). Se o EasyNetwork não estiver aberto ou em primeiro plano quando o arquivo for enviado para o computador, você receberá uma mensagem de notificação na área de notificação à direita da barra de tarefas. Clique na mensagem de notificação para abrir o EasyNetwork e acessar o arquivo.

Para receber um arquivo de outro computador:

- Clique em **Recebido** e arraste o arquivo da caixa de entrada do EasyNetwork para uma pasta no Windows Explorer.

Dica: Você também pode receber um arquivo de outro computador selecionando o arquivo na caixa de entrada do EasyNetwork e clicando em **Aceitar** no menu **Ferramentas**. Na caixa de diálogo Aceitar, navegue até a pasta em que deseja salvar os arquivos recebidos, selecione-a e clique em **Salvar**.

Receber uma notificação quando um arquivo for enviado

É possível receber uma notificação quando outro computador da rede gerenciada enviar um arquivo. Se o EasyNetwork não estiver aberto no momento ou não estiver em primeiro plano em sua área de trabalho, uma mensagem de notificação aparecerá na área de notificação, à direita da barra de tarefas do Windows.

Para receber uma notificação quando um arquivo for enviado:

1. No menu **Opções**, clique em **Configurar**.
2. Na caixa de diálogo Configurar, marque a caixa de seleção **Notificar quando algum outro computador enviar arquivos para mim**.
3. Clique em **OK**.

CAPÍTULO 22

Compartilhando impressoras

Depois que você se associa à rede gerenciada, o EasyNetwork compartilha automaticamente todas as impressoras locais conectadas ao seu computador. Ele também detecta impressoras compartilhadas por outros computadores em sua rede e permite que você configure e use essas impressoras.

Neste capítulo

Trabalhando com impressoras compartilhadas

Depois que você se associa à rede gerenciada, o EasyNetwork compartilha automaticamente todas as impressoras locais conectadas ao seu computador, usando o nome atual da impressora como nome da impressora compartilhada. Ele também detecta impressoras compartilhadas por outros computadores em sua rede e permite que você configure e use essas impressoras. Se você tiver configurado um driver de impressora para imprimir através de um servidor de impressão da rede (por exemplo, um servidor de impressão USB sem fio), o EasyNetwork considerará essa impressora como uma impressora local e a compartilhará automaticamente na rede. Também é possível parar de compartilhar uma impressora a qualquer momento.

O EasyNetwork também detecta impressoras compartilhadas por todos os outros computadores da rede. Se ele detectar uma impressora remota que ainda não esteja conectada ao seu computador, o link **Impressoras de rede disponíveis** aparecerá na janela Arquivos compartilhados quando você abrir o EasyNetwork pela primeira vez. Isso permite que você instale as impressoras disponíveis ou desinstale impressoras que já estejam conectadas ao seu computador. Também é possível atualizar a lista de impressoras detectadas na rede.

Se você ainda não se associou à rede gerenciada, mas está conectado a ela, é possível acessar as impressoras compartilhadas a partir do painel de controle padrão do Windows.

Parar de compartilhar uma impressora

É possível parar de compartilhar uma impressora a qualquer momento. Membros que instalaram a impressora não poderão mais imprimir com ela.

Para parar de compartilhar uma impressora:

1. No menu **Ferramentas**, clique em **Impressoras**.
2. Na caixa de diálogo Gerenciar impressoras da rede, clique no nome da impressora que não deseja mais compartilhar.
3. Clique em **Não compartilhar**.

Instalar uma impressora de rede disponível

Como membro de uma rede gerenciada, você pode acessar as impressoras compartilhadas na rede. Para fazer isso, instale o driver usado pela impressora. Se o proprietário da impressora parar de compartilhá-la depois da instalação, você não poderá mais imprimir com essa impressora.

Para instalar uma impressora de rede disponível:

1. No menu **Ferramentas**, clique em **Impressoras**.
2. Na caixa de diálogo Impressoras de rede disponíveis, clique em um nome de impressora.
3. Clique em **Instalar**.

CAPÍTULO 23

Referência

O Glossário de termos lista e define a terminologia de segurança usada com mais freqüência nos produtos McAfee.

A seção Sobre a McAfee fornece informações legais sobre a McAfee Corporation.

Glossário

8

802.11

Um conjunto de padrões IEEE para tecnologia de LAN sem fio. O 802.11 especifica uma comunicação pelo ar entre um cliente sem fio e uma estação base ou entre dois clientes sem fio. As várias especificações do 802.11 são: 802.11a, um padrão para comunicação em rede até 54 Mbps na banda de 5 Ghz; 802.11b, um padrão para rede até 11 Mbps na banda de 2,4 Ghz; 802.11g, um padrão para rede até 54 Mbps na banda de 2,4 Ghz; e 802.11i, um conjunto de padrões de segurança para todas as redes Ethernet sem fio.

802.11a

Uma extensão do 802.11 que se aplica a LANs sem fio e que envia dados a até 54 Mbps na banda de 5 GHz. Embora a velocidade de transmissão seja maior do que com o 802.11b, o alcance é muito menor.

802.11b

Uma extensão do 802.11 que se aplica a LANs sem fio e que permite transmissão a 11 Mbps na banda de 2,4 GHz. O 802.11b é considerado atualmente o padrão em comunicação sem fio.

802.11g

Uma extensão do 802.11 que se aplica a LANs sem fio e que permite até 54 Mbps na banda de 2,4 GHz.

802.1x

Não suportado pelo Wireless Home Network Security. Um padrão IEEE para autenticação em redes com ou sem fio, porém mais freqüentemente usado em conjunto com a rede sem fio 802.11. Esse padrão proporciona uma autenticação forte e mútua entre um cliente e um servidor de autenticação. Além disso, o 802.1x pode fornecer chaves WEP dinâmicas por usuário e por sessão, eliminando o trabalho administrativo e os riscos de segurança inerentes às chaves WEP estáticas.

A

adaptador sem fio

Contém os circuitos necessários para que um computador ou outro dispositivo se comunique com um roteador sem fio (conectado a uma rede sem fio). Os adaptadores sem fio podem ser incorporados nos circuitos principais de um dispositivo de hardware ou podem ser uma extensão avulsa a ser inserida em um dispositivo através da porta apropriada.

Análise de imagens

Impede que imagens potencialmente inapropriadas apareçam. As imagens são bloqueadas para todos os usuários, exceto membros da faixa etária adulta.

arquivamento completo

Arquivar um conjunto completo de dados com base nos tipos de arquivos e locais de observação que você configurou.

arquivamento rápido

Arquivar apenas os arquivos em observação que foram alterados desde o último arquivamento rápido ou completo.

arquivar

Criar uma cópia dos seus arquivos observados localmente na unidade USB, de CD, de DVD, de disco rígido externo ou de rede.

arquivar

Criar uma cópia dos seus arquivos observados localmente na unidade USB, de CD, de DVD, de disco rígido externo ou de rede.

ataque de dicionário

Esses ataques envolvem a tentativa de uma variedade de palavras de uma lista para descobrir a senha de alguém. Os atacantes não experimentam manualmente todas as combinações, mas possuem ferramentas que tentam automaticamente identificar uma senha.

ataque de força bruta

Também conhecido como cracking por força bruta, trata-se de um método de tentativa e erro utilizado por programas aplicativos para decodificar dados criptografados, como senhas, através de procedimentos exaustivos (ou seja, força bruta) em vez de empregar estratégias intelectuais. Assim como um criminoso pode abrir ou arrombar um cofre tentando várias combinações possíveis, um aplicativo de crack força bruta experimenta seqüencialmente todas as combinações possíveis de caracteres válidos. A força bruta é considerada uma abordagem infalível, embora demorada.

ataque man-in-the-middle (homem no meio)

O atacante intercepta mensagens em uma troca de chaves públicas e, em seguida, as retransmite, substituindo a chave requisitada pela sua própria chave pública, de maneira que as duas partes originais ainda pareçam estar se comunicando diretamente uma com a outra. O atacante usa um programa que aparenta ser o servidor para o cliente e que aparenta ser o cliente para o servidor. Esse ataque pode ser usado simplesmente para obter acesso às mensagens ou para permitir ao atacante modificá-las antes de retransmiti-las. O termo é derivado do jogo de bola no qual algumas pessoas tentam jogar uma bola diretamente de uma para outra enquanto uma pessoa no meio tenta alcançá-la.

autenticação

O processo de identificação de um indivíduo, normalmente com base em um nome de usuário e uma senha. A autenticação garante que o indivíduo é quem afirma ser, mas nada diz quanto aos direitos de acesso desse indivíduo.

B

backup

Criar uma cópia dos seus arquivos observados em um servidor on-line seguro.

biblioteca

A área de armazenamento on-line para os arquivos publicados pelos usuários do Data Backup. A biblioteca é um site na Internet, acessível a todos que tenham acesso à Internet.

cabeçalho

Cabeçalho são informações adicionadas à parte da mensagem em todo o seu ciclo de vida. O cabeçalho informa ao software de Internet como enviar a mensagem, para onde as respostas da mensagem devem ser enviadas, um identificador exclusivo para a mensagem de e-mail e outras informações administrativas. Exemplos de campos de cabeçalho: Para, De, CC, Data, Assunto, ID de mensagem e Recebido.

cavalo de Tróia

Os cavalos de Tróia são programas que fingem ser aplicativos benignos. Os cavalos de Tróia não são vírus porque não se replicam, mas podem ser tão destruidores quanto os vírus.

chave

Uma série de letras e/ou números usados por dois dispositivos para autenticar sua comunicação. Ambos os dispositivos precisam ter a chave. Consulte também WEP, WPA, WPA2, WPA-PSK e WPA2-PSK.

cliente

Um aplicativo, executado em um computador pessoal ou estação de trabalho, que depende de um servidor para executar algumas operações. Por exemplo, um cliente de e-mail é um aplicativo que permite enviar e receber e-mail.

cliente de e-mail

Uma conta de e-mail. Por exemplo, Microsoft Outlook ou Eudora.

Cofre de senhas

Uma área de armazenamento segura para suas senhas pessoais. Ele permite que você guarde suas senhas, garantindo que nenhum outro usuário (nem mesmo um Administrador McAfee ou administrador do sistema) poderá acessá-las.

compactação

Um processo através do qual os dados (arquivos) são compactados em um formato que minimiza o espaço necessário para armazená-lo ou transmiti-lo.

compartilhar

Uma operação que permite que os destinatários de e-mail acessem os arquivos com backup selecionados, por um período limitado. Ao compartilhar um arquivo, você envia a cópia de backup do arquivo para os destinatários de e-mail especificados. Os destinatários recebem uma mensagem de e-mail do Data Backup, indicando que os arquivos foram compartilhados com eles. O e-mail também contém um link para os arquivos compartilhados.

conta de e-mail padrão

A maioria dos usuários domésticos usa este tipo de conta. Consulte também conta POP3.

conta MAPI

Acrônimo para Messaging Application Programming Interface (interface de programação de aplicativos de mensagens). A especificação de interface da Microsoft que permite que diferentes aplicativos de mensagens e de grupos de trabalho (incluindo e-mail, correio de voz ou fax) funcionem através de um único cliente, como o cliente Exchange. Por isso, normalmente o MAPI é usado em ambientes corporativos quando a empresa possui o Microsoft® Exchange Server. Porém, muitas pessoas usam o Microsoft Outlook como e-mail pessoal da Internet.

conta MSN

Acrônimo para Microsoft Network. Um serviço on-line e portal de Internet. Essa é uma conta com base na Web.

conta POP3

Acrônimo para Post Office Protocol 3. A maioria dos usuários domésticos possuem esse tipo de conta. Essa é a versão atual do padrão Post Office Protocol em uso comum nas redes TCP/IP. Também conhecida como conta de e-mail padrão.

controles pelos pais

Configurações que permitem que você configure as classificações de conteúdo, que restringem os sites e o conteúdo que um usuário pode exibir, bem como os limites de horário da Internet, que especificam o período e a duração do horário em que um usuário pode acessar a Internet. Eles também permitem que você restrinja universalmente o acesso a sites da Web específicos, além de conceder e bloquear o acesso com base em faixa etária e palavras-chave associadas.

cookie

Na World Wide Web, um bloco de dados que um servidor Web armazena em um sistema do cliente. Quando um usuário retorna ao mesmo site da Web, o navegador envia uma cópia do cookie de volta para o servidor. Os cookies são usados para identificar usuários, instruir o servidor a enviar uma versão personalizada da página da Web solicitada, submeter informações da conta para o usuário, e para outras finalidades administrativas.

Os cookies permitem que o sites memorizem quem é você e controlem quantas pessoas visitaram o site, quando visitaram e quais páginas foram exibidas. Os cookies também ajudam uma empresa a personalizar seu site da Web. Muitos sites da Web exigem um nome de usuário e senha para o acesso a determinadas páginas, e enviam um cookie ao seu computador para que você não precise fazer logon a cada visita. No entanto, os cookies podem ser usados com fins maliciosos. As empresas de propaganda on-line freqüentemente usam cookies para determinar quais sites você visita com mais freqüência e colocam anúncios em seus sites favoritos. Antes de aceitar os cookies de um site, verifique se ele é confiável.

Embora sejam uma fonte de informações para empresas legítimas, os cookies também podem ser uma fonte de informações para hackers. Muitos sites com lojas on-line armazenam informações de cartões de crédito e outras informações pessoais em cookies para facilitar as compras. Infelizmente, pode haver falhas de segurança que permitam o acesso dos hackers às informações dos cookies armazenados nos computadores dos clientes.

criptografia

Um processo através do qual os dados são transformados de texto para código, ocultando as informações para que fiquem ilegíveis para as pessoas que não sabem descriptografá-las.

D

disco rígido externo

Uma unidade de disco rígido é armazenada fora do gabinete do computador.

DNS

Acrônimo para Domain Name System (sistema de nomes de domínios). O sistema hierárquico através do qual os hosts na Internet possuem endereços de nome de domínio (como bluestem.prairienet.org) e endereços IP (como 192.17.3.4). O endereço de nome de domínio é usado por usuários humanos e é automaticamente convertido no endereço IP numérico, que é usado pelo software de roteamento de pacotes. Os nomes DNS consistem em um domínio de nível superior (como: .com, .org e .net), um domínio de nível secundário (o nome do site de uma empresa, organização ou indivíduo), e possivelmente um ou mais subdomínios (servidores dentro de um domínio de nível secundário). Consulte também servidor DNS e endereço IP.

domínio

Um endereço de uma conexão de rede que identifica o proprietário desse endereço em um formato hierárquico: server.organization.type. Por exemplo, www.whitehouse.gov identifica o servidor da Web na Casa Branca, que faz parte do governo dos EUA.

E

e-mail

Correio eletrônico, mensagens enviadas através da Internet ou dentro de uma LAN ou WAN corporativa. Anexos de e-mail na forma de arquivos executáveis (EXE) ou VBS (scripts Visual Basic) tornaram-se muito populares como forma de transmissão de vírus e cavalos de Tróia.

Endereço IP

O endereço Internet Protocol ou o endereço IP é um número exclusivo composto por quatro partes separadas por pontos (p. ex. 63.227.89.66). Todos os computadores da Internet, dos maiores servidores a um laptop, que se comunicam através de um telefone celular, têm um número IP exclusivo. Nem todos os computadores têm um nome de domínio, mas todos têm um IP.

Os itens a seguir listam alguns tipos de endereço IP incomuns:

- Endereços IP não roteáveis: Também conhecidos como Espaço IP privado. São endereços IP que não podem ser usados na Internet. Os blocos de endereços IP privados são 10.x.x.x, 172.16.x.x - 172.31.x.x e 192.168.x.x.
- Endereços IP de Loopback**:** Os endereços de loopback são usados para teste. O tráfego enviado a esse bloco de endereços IP volta para o dispositivo que gerou o pacote. Ele

nunca sai do dispositivo, sendo usado principalmente para testes de hardware e software. O bloco de endereços IP de loopback é 127.x.x.x.

Endereço IP nulo: É um endereço IP inválido. Quando visualizado, ele indica que o tráfego tinha um endereço IP em branco. Obviamente, isso não é normal e geralmente indica que o remetente está escondendo a origem do tráfego. O remetente não poderá receber nenhuma resposta para esse tráfego, a não ser que o pacote seja recebido por um aplicativo que reconheça seu conteúdo e que o pacote contenha instruções específicas para esse aplicativo. Qualquer endereço iniciado com 0 (0.x.x.x) é um endereço nulo. Por exemplo, 0.0.0.0 é um endereço IP nulo.

Endereço MAC (Media Access Control)

Um endereço de baixo nível atribuído ao dispositivo físico que acessa a rede.

ESS (Extended Service Set)

Um conjunto de duas ou mais redes que formam uma única sub-rede.

estação

Um único computador conectado a uma rede.

evento

Eventos de 0.0.0.0

Se você vir eventos de endereços IP 0.0.0.0, há duas possíveis causas. A primeira, e mais comum, é que por algum motivo o computador recebeu um pacote mal formatado. A Internet não é cem por cento confiável, e podem ocorrer pacotes ruins. Como o Firewall vê os pacotes antes que o TCP/IP possa validá-los, ele pode relatar esses pacotes como um evento.

A segunda situação ocorre quando o IP de origem é fraudado ou falso. Pacotes fraudados podem ser um sinal de que alguém está procurando por cavalos de Tróia e tentou fazê-lo em seu computador. É importante se lembrar de que o Firewall bloqueia a tentativa.

Eventos de 127.0.0.1

Às vezes, os eventos indicam o IP de origem como 127.0.0.1. É importante observar que esse IP é especial e é conhecido como endereço de loopback.

Independentemente de qual computador você esteja usando, 127.0.0.1 sempre se refere ao seu computador local. Esse endereço também é chamado de host local, pois o host local de nome de computador sempre será convertido novamente no endereço IP 127.0.0.1. Isso significa que o computador está tentando invadir ele mesmo? Algum Cavalo de Tróia ou spyware está tentando tomar o controle de seu computador? Provavelmente não. Muitos programas legítimos usam o endereço de loopback para comunicação entre componentes. Por exemplo, muitos servidores de e-mail pessoal ou servidores Web podem ser configurados através de uma interface da Web que geralmente é acessada através de um endereço semelhante a http://localhost/.

Contudo, o Firewall permite o tráfego desses programas; portanto, se você vir eventos de 127.0.0.1, isso geralmente significa que o endereço IP de origem foi fraudado ou é falso. Os pacotes fraudados geralmente são um sinal de que alguém está fazendo uma varredura em busca de Cavalos de Tróia. É importante se lembrar de que o Firewall bloqueia essa tentativa. Evidentemente, relatar eventos de 127.0.0.1 não será útil; portanto, não há necessidade de tal procedimento.

Assim sendo, alguns programas, particularmente o Netscape 6.2 e posteriores, exigem que o endereço 127.0.0.1 seja adicionado à lista **Endereços IP confiáveis**. Os componentes desses programas se comunicam entre si de uma maneira que impede que o Firewall determine se o tráfego é local.

No exemplo do Netscape 6.2, se você não confiar no 127.0.0.1, não poderá usar a sua lista de amigos. Portanto, se você receber tráfego de 127.0.0.1 e todos os programas do computador funcionarem normalmente, é sinal de que esse tráfego pode ser bloqueado sem problemas. No entanto, se um programa (como o Netscape) estiver com problemas, adicione 127.0.0.1 à lista **Endereços IP confiáveis** no Firewall e, em seguida, veja se o problema foi resolvido.

Se a inserção de 127.0.0.1 na lista **Endereços IP confiáveis** corrigir o problema, será necessário considerar as seguintes opções: se confiar no 127.0.0.1, o programa funcionará, mas você estará mais vulnerável a ataques de fraude. Se você não confiar no endereço, o programa não funcionará, mas você continuará protegido contra qualquer tráfego mal-intencionado.

Eventos de computadores na LAN

Para a maioria das configurações de LAN corporativas, você pode confiar em todos os computadores na sua LAN.

Eventos de endereços IP privados

Os endereços IP de formato 192.168.xxx.xxx, 10.xxx.xxx.xxx e 172.16.0.0 - 172.31.255.255 são chamados de não-roteáveis ou privados. Esses endereços IP nunca devem sair da sua rede e, na maioria das vezes, são confiáveis.

O bloco 192.168 é usado com o Microsoft Internet Connection Sharing (ICS). Se você estiver usando ICS e vir eventos desse bloco de IP, poderá adicionar o endereço IP 192.168.255.255 à sua lista **Endereços IP confiáveis**. Isso tornará todo o bloco 192.168.xxx.xxx confiável.

Se você não estiver em uma rede privada e receber eventos desses intervalos de endereços IP, talvez o endereço IP de origem seja fraudado ou falso. Pacotes fraudados são, em geral, sinal de que alguém está em busca de cavalos de Tróia. É importante se lembrar de que o Firewall bloqueia essa tentativa.

Como os endereços IP privados são separados dos endereços IP da Internet, relatar esses eventos não causa nenhum efeito.

falsificação de IP

Consiste em forjar o endereço IP de um pacote IP. Isso é usado em diversos tipos de ataque, incluindo seqüestro de sessão. Também é freqüentemente utilizado para falsificar os cabeçalhos de e-mail de SPAM para impedir que sejam rastreados corretamente.

firewall

Um sistema desenvolvido para impedir o acesso não autorizado a uma rede privada ou a partir de uma rede privada. Os firewalls podem ser implementados tanto em hardware quanto em software, ou como uma combinação de ambos. Firewalls são freqüentemente utilizados para impedir usuários da Internet não autorizados de acessarem redes privadas conectadas à Internet, especialmente intranets. Todas as mensagens que entram e que saem da intranet passam pelo firewall. O firewall examina cada mensagem e bloqueia as que não satisfazem os critérios de segurança especificados. O firewall é considerado a primeira linha de defesa na proteção de informações privadas. Para maior segurança, os dados podem ser criptografados.

gateway integrado

Um dispositivo que combina as funções de um ponto de acesso (PA), roteador e firewall. Alguns dispositivos também podem incluir aperfeiçoamentos de segurança e recursos de ponte.

grupos de classificação de conteúdo

Faixa etária à qual um usuário pertence. O conteúdo é classificado (ou seja, disponibilizado ou bloqueado) com base no grupo de classificação de conteúdo ao qual o usuário pertence. Os grupos de classificação de conteúdo incluem: crianças pequenas, crianças, pré-adolescentes, adolescentes e adultos.

hotspot

Um local físico específico no qual um ponto de acesso (PA) oferece serviços públicos de rede sem fio em banda larga para visitantes móveis através de uma rede sem fio. Os hotspots costumam estar situados em locais com alta concentração de pessoas, como aeroportos, estações de trens, bibliotecas, marinas, centros de convenções e hotéis. Eles normalmente têm um alcance curto.

Internet

A Internet é composta por um grande número de redes interconectadas que usam protocolos TCP/IP para a localização e a transferência de dados. A Internet surgiu como uma rede criada para ligar computadores de universidades e faculdades (no fim da década de 60 e começo de 70), fundada pelo Departamento de Defesa dos EUA e era chamada ARPANET. A Internet hoje é uma rede global de quase 100.000 redes independentes.

intranet

Uma rede privada, geralmente dentro de uma organização, que funciona de forma muito semelhante à Internet. Agora é prática comum conceder acesso às intranets para computadores independentes usados por alunos ou funcionários remotos. Firewalls, procedimentos de logon e senhas são usados para oferecer segurança.

LAN (Local Area Network)

Uma rede de computadores que se estende por uma área relativamente pequena. A maioria das LANs se restringe a um mesmo edifício ou grupo de edifícios. No entanto, uma LAN pode ser conectada a outras LANs a qualquer distância, via telefone ou ondas de rádio. Um sistema de LANs conectadas dessa forma é o que se chama de rede de longa distância (WAN, wide-area network). A maioria das LANs conectam estações de trabalho e computadores pessoais, geralmente através de hubs ou switches simples. Cada nó (computador individual) de uma LAN possui sua própria CPU, com a qual executa programas, mas também é capaz de acessar dados e dispositivos (como, por exemplo, impressoras) em qualquer lugar da LAN. Isso significa que vários usuários podem compartilhar dispositivos caros, como impressoras a laser, bem como dados. Os usuários também podem usar a LAN para se comunicar uns com os outros, por exemplo, enviando e-mail ou entrando em sessões de chat.

largura de banda

A quantidade de dados que podem ser transmitidos em um determinado período de tempo. Em dispositivos digitais, a largura de banda costuma ser expressa em bits por segundo (bps) ou em bytes por segundo. Em dispositivos analógicos, a largura de banda é expressa em ciclos por segundo ou Hertz (Hz).

lista branca

Uma lista de sites da Web que possuem permissão para serem acessados, por não serem considerados fraudulentos.

lista negra

Uma lista de sites da Web considerados mal intencionados. Um site da Web pode ser colocado em uma lista negra por ser uma operação fraudulenta ou por explorar a vulnerabilidade do navegador para enviar programas potencialmente indesejados ao usuário.

locais de observação

As pastas no seu computador monitoradas pelo Data Backup.

locais de observação superficial

Uma pasta em seu computador na qual as alterações são monitoradas pelo Data Backup. Se você configurar um local de observação superficial, o Data Backup fará backup dos tipos de arquivos em observação dentro dessa pasta, mas não incluirá suas subpastas.

local de observação detalhada

Uma pasta (e todas as subpastas) em seu computador na qual as alterações são monitoradas pelo Data Backup. Se você definir um local de observação detalhada, o Data Backup fará backup dos tipos de arquivos em observação dentro dessa pasta e de suas subpastas.

MAC (Media Access Control ou Message Authenticator Code)

Quanto ao primeiro, consulte Endereço MAC. O segundo é um código utilizado para identificar uma determinada mensagem (por exemplo, uma mensagem RADIUS). O código é geralmente uma mistura criptografada do conteúdo da mensagem, incluindo um valor exclusivo para proporcionar uma proteção contra reprodução.

mapa de rede

No Network Manager, uma representação gráfica dos computadores e componentes que fazem parte de uma rede doméstica.

navegador

Um programa cliente que usa o Hypertext Transfer Protocol (HTTP) para fazer solicitações de servidores Web na Internet. Um navegador da Web exibe o conteúdo de forma gráfica para o usuário.

Negação de serviço

Na Internet, um ataque de negação de serviço (DoS, denial of service) é um incidente no qual um usuário ou organização é privado dos serviços ou de um recurso que, em condições normais, estaria disponível. Tipicamente, a perda de serviços consiste na indisponibilidade de um determinado serviço de rede, como o e-mail, ou a perda temporária de todos os serviços e da conectividade de rede. Nos piores casos, por exemplo, um site acessado por milhões de pessoas pode, ocasionalmente, ser forçado a interromper temporariamente sua operação. Um ataque de negação de serviço também pode destruir a programação e os arquivos de um sistema de computador. Embora normalmente seja proposital e mal-intencionado, um ataque de negação de serviço pode, às vezes, ocorrer acidentalmente. Um ataque de negação de serviço é um tipo de violação de segurança em sistemas de computadores que não costuma resultar em roubo de informações ou em outras perdas de segurança. No entanto, esses ataques podem custar bastante tempo e dinheiro à pessoa ou empresa atingida.

NIC (Network Interface Card)

Uma placa que se conecta a um laptop ou a algum outro dispositivo e que conecta esse dispositivo à LAN.

palavra-chave

Um palavra que você pode atribuir a um arquivo com backup para estabelecer um relacionamento ou conexão com outros arquivos que possuam a mesma palavra-chave atribuída. Atribuir as palavras-chaves aos arquivos facilita a pesquisa pelos arquivos que você publicou na Internet.

phishing

Pronuncia-se "fishing", trata-se de uma fraude para roubar informações valiosas, como números de cartão de crédito e números de CPF, IDs de usuário e senha. Um e-mail aparentemente oficial é enviado a vítimas em potencial, fingindo ser de seus provedores de Internet, de bancos ou de lojas. Os e-mails podem ser enviados a pessoas em listas selecionadas ou em qualquer lista, esperando que alguma porcentagem dos destinatários tenha realmente uma conta na organização real.

placas adaptadoras sem fio PCI

Conecta um computador desktop a uma rede. A placa se conecta em um slot de expansão PCI dentro do computador.

placas adaptadoras sem fio USB

Oferece uma interface serial Plug and Play expansível. Essa interface proporciona uma conexão padrão sem fio e de baixo custo para dispositivos periféricos, como teclados, mouses, joysticks, impressoras, scanners, dispositivos de armazenamento e câmeras de videoconferência.

Ponto de acesso (PA)

Um dispositivo de rede que possibilita que clientes 802.11 se conectem a uma rede local (LAN). Os PAs estendem o alcance físico do serviço para usuários sem fio. Eles são ocasionalmente chamados de roteadores sem fio.

pontos de acesso ilícitos

Um ponto de acesso que uma empresa não autoriza para operação. O problema é que os pontos de acesso ilícitos normalmente não estão em conformidade com as políticas de segurança de LAN sem fio (WLAN). Um ponto de acesso ilícito permite uma interface aberta e desprotegida com a rede corporativa, partindo de fora do perímetro controlado fisicamente.

Dentro de uma WLAN devidamente protegida, pontos de acesso ilícitos são mais prejudiciais que usuários ilícitos. Usuários não autorizados tentando obter acesso a uma WLAN provavelmente não conseguirão atingir recursos corporativos valiosos se mecanismos de autenticação eficazes estiverem implementados. No entanto, problemas graves podem ocorrer quando um funcionário ou hacker se conecta a um ponto de acesso ilícito. Tal ponto de acesso permite que praticamente qualquer pessoa que tenha um dispositivo equipado com 802.11 entre na rede corporativa. Isso os coloca muito próximos a recursos de importância crucial.

pop-ups

Pequenas janelas que aparecem sobre outras janelas na tela de seu computador. As janelas pop-up geralmente são usadas nos navegadores da Web para exibir anúncios. A McAfee bloqueia as janelas pop-up que são carregadas automaticamente quando uma página da Web é carregada no navegador. As janelas pop-up que são carregadas quando você clica em um link não são bloqueadas pela McAfee.

porta

Local por onde as informações passam para entrar ou sair de um computador; por exemplo, um modem analógico convencional está conectado a uma porta serial. Os números de porta em comunicações TCP/IP são valores virtuais usados para separar tráfego em fluxos específicos de aplicativos. Portas são atribuídas a protocolos padrão como SMTP ou HTTP para que os programas saibam quais portas usar para tentar uma conexão. A porta de destino para pacotes TCP indica o aplicativo ou servidor procurado.

PPPoE

Point-to-Point Protocol Over Ethernet, um protocolo de comunicação. Usado por muitos provedores DSL, o PPPoE suporta a autenticação e as camadas de protocolo amplamente utilizadas no PPP, permitindo estabelecer uma conexão ponto a ponto na arquitetura habitualmente multiponto Ethernet.

programa potencialmente indesejado

Os programas potencialmente indesejados incluem spyware, adware e outros programas que coletam e transmitem seus dados sem a sua permissão.

protocolo

Um formato padronizado para transmissão de dados entre dois dispositivos. Do ponto de vista do usuário, o único aspecto interessante dos protocolos é que o computador ou dispositivo em questão precisa ter suporte para os protocolos apropriados, caso queira se comunicar com outros computadores. O protocolo pode ser implementado em hardware ou em software.

proxy

Um computador (ou software executado nele) que funciona como uma barreira entre uma rede e a Internet, apresentando somente um único endereço de rede para sites externos. Ao atuar como intermediário representando todos os computadores internos, o proxy protege identidades de rede ao mesmo tempo que oferece acesso à Internet. Consulte também servidor proxy.

publicar

Disponibilizar publicamente um arquivo com backup, na Internet.

quarentena

Quando arquivos suspeitos são detectados, eles ficam em quarentena. Em seguida, você pode executar a ação apropriada.

RADIUS (Remote Access Dial-In User Service)

Um protocolo que proporciona autenticação de usuários, normalmente numa situação de acesso remoto. Originalmente definido para uso com servidores de acesso remoto discado, o protocolo é atualmente usado em uma variedade de ambientes de autenticação, incluindo a autenticação 802.1x do segredo compartilhado do usuário de uma WLAN.

rede

Quando você conecta dois ou mais computadores, cria uma rede.

rede gerenciada

Uma rede doméstica gerenciada com dois tipos de membros: membros gerenciados e não gerenciados. Membros gerenciados permitem que outros computadores da rede monitores seu status de proteção McAfee, enquanto membros não gerenciados não o permitem.

repositório de backup on-line

O local no servidor on-line no qual seus arquivos de observação são armazenados depois de serem submetidos ao backup.

restaurar

Recuperar uma cópia de um arquivo a partir do arquivamento ou do repositório online de backup.

roaming

A capacidade de se passar da área de cobertura de um PA para a área de outro sem interrupção do serviço ou perda de conectividade.

roteador

Um dispositivo de rede que encaminha pacotes de uma rede para outra. Com base em tabelas de roteamento internas, os roteadores lêem cada pacote recebido e determinam como encaminhá-lo. A interface do roteador para a qual os pacotes transmitidos são enviados pode ser determinada por qualquer combinação de endereços de origem e de destino, bem como condições de tráfego atuais, como carga, custos das linhas ou linhas ruins. Os roteadores são, às vezes, chamados de pontos de acesso (PA).

script

Os scripts podem criar, copiar ou excluir arquivos. Eles também podem abrir o seu registro do Windows.

segredo compartilhado

Consulte também RADIUS. Protege partes sigilosas de mensagens RADIUS. Esse segredo compartilhado é uma senha compartilhada entre o autenticador e o servidor de autenticação de alguma maneira segura.

senha

Um código (geralmente alfanumérico) usado para obter acesso ao computador ou a um determinado programa ou site da Web.

servidor

Computador ou software que oferece serviços específicos a softwares em execução em outros computadores. O "servidor de email" de seu ISP é um software que lida com todas as mensagens enviadas e recebidas de todos os usuários. Um servidor em uma LAN é um hardware que constitui o principal nó da rede. Ele também pode conter softwares que oferecem serviços específicos, dados ou outros recursos a todos os computadores clientes a ele conectados.

servidor DNS

Abreviação para o servidor do Sistema de nomes de domínios. Um computador que pode responder a perguntas do Sistema de nomes de domínios (DNS). O servidor DNS mantém um banco de dados de computadores host e seus endereços IP correspondentes. A receber o nome apex.com, por exemplo, o servidor DNS retornaria o endereço IP da empresa hipotética Apex. Também denominado: servidor de nomes. Consulte também DNS e endereço IP.

Servidor proxy

Um componente de firewall que gerencia o tráfego da Internet de e para uma rede local (LAN). Um servidor proxy pode melhorar o desempenho ao oferecer dados solicitados com freqüência, como uma página popular da Web, e pode filtrar e descartar solicitações que o proprietário não considera apropriadas, como solicitações de acesso não autorizado a arquivos patenteados.

servidor SMTP

Acrônimo para Simple Mail Transfer Protocol (protocolo de transferência de correio simples). Um protocolo TCP/IP para enviar mensagens de um computador a outro em uma rede. Esse protocolo é usado na Internet para rotear o e-mail.

sincronizar

Resolver as inconsistências entre os arquivos do backup e os armazenados em seu computador local. Os arquivos são sincronizados quando a versão do arquivo no repositório on-line de backup for mais recente que a versão do arquivo em outros computadores. A sincronização atualiza a cópia do arquivo em seus computadores com a versão do arquivo no repositório de backup on-line.

sobrecarga de buffer

Sobrecargas de buffer ocorrem quando programas ou processos suspeitos tentam armazenar dados em um buffer (área de armazenagem temporária de dados) além de seu limite, corrompendo ou sobrescrevendo dados válidos em buffers adjacentes.

SSID (Service Set Identifier)

Nome de rede para os dispositivos de um subsistema de LAN sem fio. Trata-se de uma seqüência de 32 caracteres de texto simples acrescentada ao cabeçalho de todo pacote WLAN. O SSID diferencia uma WLAN de outra, portanto, todos os usuários de uma rede precisam fornecer o mesmo SSID para ter acesso a um determinado PA. Um SSID impede o acesso de qualquer dispositivo cliente que não tenha o SSID. Contudo, o ponto de acesso (PA) divulga, por padrão, seu SSID ao se anunciar. Mesmo que a divulgação de SSID esteja desativada, um hacker pode detectar o SSID através de farejamento (sniffing).

SSL (Secure Sockets Layer)

Um protocolo desenvolvido pela Netscape para transmissão de documentos privados pela Internet. A SSL funciona utilizando uma chave pública para criptografar dados que é transferida através da conexão SSL. Tanto o Netscape Navigator quanto o Internet Explorer usam e suportam SSL, e muitos sites usam esse protocolo para obter informações confidenciais do usuário, como números de cartão de crédito. Por uma questão de convenção, os URLs que exigem uma conexão SSL começam com https: em vez de http:

SystemGuard

Os SystemGuards detectam alterações não autorizadas em seu computador e alertam você quando elas ocorrem.

texto codificado

Dados que foram criptografados. O texto codificado é ilegível até ser convertido em texto simples (descriptografado) com uma chave.

texto simples

Qualquer mensagem que não esteja criptografada.

tipos de arquivos observados

Os tipos de arquivos (por exemplo, .doc, .xls e assim por diante) que o Data Backup submete a backup ou arquiva dentro dos locais de observação.

TKIP (Temporal Key Integrity Protocol)

Uma correção rápida para superar as vulnerabilidades inerentes à segurança WEP, especialmente a reutilização de chaves de criptografia. O TKIP altera as chaves temporais a cada 10.000 pacotes, proporcionando um método de distribuição dinâmico que melhora significativamente a segurança da rede. O processo (de segurança) TKIP começa com uma chave temporal de 128 bits compartilhada entre clientes e pontos de acesso (PAs). O TKIP combina a chave temporal com o endereço MAC (da máquina cliente) e, em seguida, adiciona um vetor de inicialização relativamente grande de 16 octetos para produzir a chave que criptografa os dados. Esse procedimento garante que cada estação utilize fluxos de chaves diferentes para criptografar os dados. O TKIP usa RC4 para realizar a criptografia. A WEP também usa RC4.

unidade de rede

Uma unidade de disco ou de fita que é conectada a um servidor em uma rede compartilhada por vários usuários. Às vezes, as unidades de rede são denominadas unidades remotas.

URL

Uniform Resource Locator (URL - Localizador Uniforme de Recursos). É o formato padrão para endereços da Internet.

varredura em tempo real

É feita a varredura nos arquivos em busca de vírus e outras atividades quando eles forem acessados por você ou por seu computador.

VPN (Virtual Private Network (Rede virtual privada))

Uma rede construída pela utilização de cabeamento público para reunificar nós. Existem, por exemplo, vários sistemas que permitem criar redes utilizando a Internet como meio para transporte de dados. Esses sistemas utilizam criptografia e outros mecanismos de segurança para garantir que somente usuários autorizados possam ter acesso à rede e que os dados não possam ser interceptados.

wardriver

Pessoas munidas de laptops, software especial e algum hardware alternativo que circulam de carro por cidades, bairros e estacionamentos de empresas com o objetivo de interceptar tráfego de LAN sem fio.

Web bugs

Arquivos gráficos pequenos que podem ser incorporados em suas páginas HTML e que permitem que uma origem não autorizada configure os cookies em seu computador. Esses cookies podem então transmitir as informações para a origem não autorizada. Os Web bugs também são denominados beacons da Web, marcas de pixel, GIFs de limpeza ou GIFs invisíveis.

WEP (Wired Equivalent Privacy)

Um protocolo de criptografia e autenticação definido como parte do padrão 802.11. Suas versões iniciais baseiam-se em codificadores RC4 e possuem vulnerabilidades significativas. A WEP tenta proporcionar segurança criptografando os dados através de ondas de rádio, para que eles estejam protegidos ao serem transmitidos de um ponto para outro. No entanto, descobriu-se que a WEP não é tão segura quanto se acreditava.

Wi-Fi (Wireless Fidelity)

Termo utilizado genericamente em referência a qualquer tipo de rede 802.11, seja 802.11b, 802.11a, banda dupla, etc. O termo é empregado pela Wi-Fi Alliance.

Wi-Fi Alliance

Uma organização composta pelos maiores fornecedores de software e equipamentos de comunicação sem fio com o objetivo de (1) certificar todos os produtos com base no 802.11 quanto a interoperabilidade e (2) promover o termo Wi-Fi como marca global em todos os mercados para qualquer produto de LAN sem fio com base no 802.11. A organização atua como associação, laboratório de testes e agência reguladora para fornecedores que queiram promover a interoperabilidade e o crescimento da indústria.

Embora todos os produtos 802.11a/b/g sejam chamados Wi-Fi, somente produtos que tenham passado pelos testes da Wi-Fi Alliance podem ser denominados Wi-Fi Certified (uma marca registrada). Os produtos que são aprovados devem levar um selo de identificação em suas embalagens dizendo Wi-Fi Certified e que indique a banda de freqüências de rádio utilizada. Esse grupo era conhecido como Wireless Ethernet Compatibility Alliance (WECA), mas mudou de nome em outubro de 2002 para refletir melhor a marca Wi-Fi que desejava construir.

Wi-Fi Certified

Quaisquer produtos testados e aprovados como Wi-Fi Certified (uma marca registrada) pela Wi-Fi Alliance são certificados quanto a interoperabilidade mútua, mesmo que sejam de fabricantes diferentes. Um usuário com um produto Wi-Fi Certified pode usar qualquer marca de ponto de acesso (PA) com qualquer outra marca de hardware cliente que também seja certificado. Geralmente, porém, qualquer produto Wi-Fi que utilize a mesma freqüência de rádio (por exemplo, 2,4 GHz para 802.11b ou 11g e 5 GHz para 802.11a) funciona com outro, mesmo que não seja Wi-Fi Certified.

WLAN (Wireless Local Area Network)

Consulte também LAN. Uma rede local que utiliza um meio sem fio para conexão. Uma WLAN usa ondas de rádio de alta freqüência em vez de fios para comunicação entre os nós.

worm

Um worm é um vírus que se replica automaticamente na memória ativa e que pode enviar cópias de si mesmo através de mensagens de e-mail. Os worms replicam e consomem recursos do sistema, reduzindo o desempenho ou interrompendo as tarefas.

WPA (Wi-Fi Protected Access)

Um padrão de especificação que aumenta muito o nível de proteção de dados e controle de acesso para sistemas de LAN sem fio futuros e existentes. Desenvolvido para ser executado em hardware existente ou como uma atualização de software, o WPA é derivado do padrão IEEE 802.11i, sendo compatível com este. Quando instalado corretamente, proporciona aos usuários de LAN sem fio um elevado grau de garantia de que seus dados permaneçam protegidos e que apenas usuários de rede autorizados tenham acesso à rede.

WPA-PSK

Um modo especial de WPA desenvolvido para usuários domiciliares que não precisam de uma segurança tão forte quanto a de empresas e que não têm acesso a servidores de autenticação. Nesse modo, o usuário domiciliar digita manualmente a senha inicial para ativar o Wi-Fi Protected Access (WPA) em modo pré-compartilhado (Pre-Shared Key ou PSK), devendo ele próprio alterar a frase de senha de cada computador e ponto de acesso sem fio regularmente. Consulte também WPA2-PSK e TKIP.

WPA2

Consulte também WPA. WPA2 é uma atualização do padrão de segurança WPA e é baseada no padrão 802.11i IEEE.

WPA2-PSK

Consulte também WPA-PSK e WPA2. WPA2-PSK é semelhante ao WPA-PSK e é baseado no padrão WPA2. Um recurso comum do WPA2-PSK é que os dispositivos geralmente suportam vários modos de criptografia (por exemplo, AES, TKIP) simultaneamente, enquanto os dispositivos mais antigos geralmente suportavam apenas em um único modo de criptografia por vez (ou seja, todos os clientes teriam que usar o mesmo modo de criptografia).

Sobre a McAfee

A McAfee, Inc., com sede em Santa Clara, Califórnia, e líder mundial em prevenção de invasões e gerenciamento de riscos à segurança, fornece soluções e serviços proativos comprovados que protegem sistemas e redes em todo o mundo. Com sua experiência inigualável em segurança e compromisso com a inovação, a McAfee confere a usuários domésticos, empresas públicas e privadas, e provedores de serviços a capacidade de bloquear ataques, evitar problemas e rastrear e aprimorar continuamente sua segurança.

Copyright

Índice

D

E